GRIFS
Building the Global RFID Standards Forum

SEVENTH FRAMEWORK PROGRAMME

Project no. 215224

GRIFS

Global RFID Forum for Standards

Instrument: **Coordination and Support Action**

Thematic Priority: **Information Society Technologies**

D1.5 RFID Standardisation State of the art report - Version 3

Due date of deliverable: **2009-11-31**
Actual submission date: **2010-01-31**

Start date of project: **1 January 2008** Duration: **Two years**

Organisation name of lead contractor for this deliverable: **CEN**
Authors: Paul Chartier, Praxis Consultants,
Gertjan van den Akker, NEN

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of contents

1 Task definition and approach to the research

1.1 Terms of reference

GRIFS ("Global RFID Interoperability Forum for Standards") is a FP7 co-ordination and support action with participation of GS1, ETSI and CEN to improve collaboration in RFID standardisation and thereby to improve the global consistency of RFID standards.

The first task under the GRIFS project is to produce an overview report providing an inventory/state of the art on the development and implementation of RFID-related standards, on a global scale, identifying the standards bodies, the geographical and technical scope of the work, opportunities and risks of collaboration, including gap/overlap analysis.

"RFID" should be considered in the broadest sense, including data access and network design. However, the scope of the report will be limited to physical objects / supply chains.

The analysis will include material available from standards bodies, Governments, companies, broken down by subject area and standards bodies, and including information on the status of the standard (work item, draft, published, etc). The report will contain a (non-exhaustive) list of possibly relevant standards topic areas and standards bodies/groups to be included.

CEN is responsible for this task within the consortium and made use of 2 sub-contractors to produce the draft report. In the production of this report, both sub-contractors received also input from technical experts participating in the two other consortium partners, GS1 and ETSI.

This is the final report on standards under the GRIFS project. It is an update of the report published in November 2008.

1.2 The RFID architecture model

1.2.1 The core architecture

RFID standards are already published or being developed to cover aspects of an RFID system from the tag through to data exchange with business partners. Details are discussed in Clause 7. Figure 1 shows a comprehensive RFID system architecture, the components of which are discussed in Clause 7.

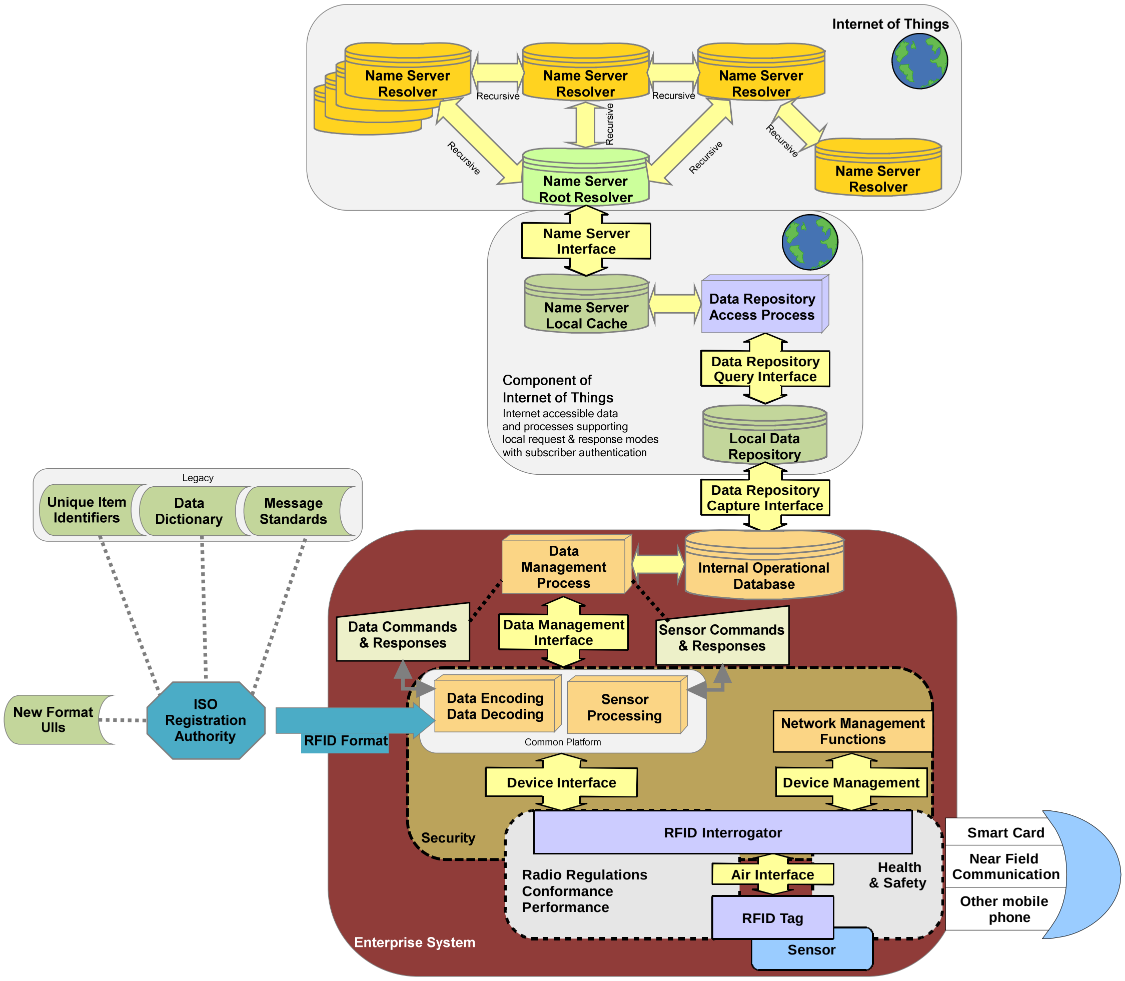


Figure 1: RFID system architecture

Some of the standards in the architecture are still in a development phase, so there might be changes in future. For example, ISO had an application interface standard in place at the beginning of the GRIFS project; this has now been withdrawn.

No application currently uses all the components, even of standards that have been published.

We have sub-divided the architecture into four component parts:

- The enterprise system, dealing with all aspects where RFID as a data carrier is used to assist with some functional aspects of business or commercial operations.
- Internet-based data exchange components that are internal to the enterprise.
- Internet-based data exchange that is external with partners and other stakeholders.
- The ISO Registration Authority for data format that provides support for conversion legacy data and for new forms of unique item identifiers.

1.2.2 The network of influencing factors

A major part of the GRIFS project is to identify potential standards development areas where collaboration between standards development organizations could reduce some unnecessary work, and even reduce potential conflict between apparent overlapping work. To address this, we have developed a simple network model that has two major hubs. One of the hubs is RFID data capture, effectively dealing with technology aspects; and the other hub is RFID data process, effectively dealing with the information flow. Figure 2 identifies various developments that we consider might impact on the development of RFID standards.

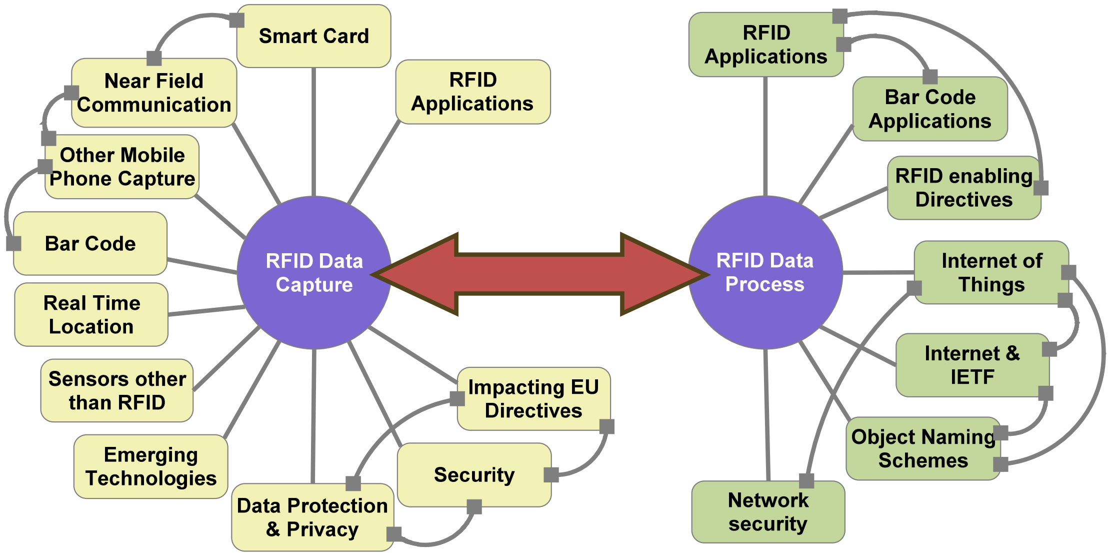


Figure 2: Network of influencing developments

Most of the links are fairly explanatory, but we provide the following brief synopsis of their relationship below. The relationships with RFID data capture are:

- **RFID applications**: The technology has to be able to support specific application requirements and, until recently, some air interfaces provided too little memory for some applications.
- **Smart card**: This matters because smart card technology shares features of the 13.56MHz air interface, and with new developments with each technology greater understanding is required.
- **Near Field Communication**: As this is intended to use 13.56 MHz technology, including some of the smart card technology, there is an obvious overlap.
- **Other mobile phone capture**: In addition to the NFC Forum work at 13.56 MHz, other work in ISO is taking place at different RFID frequencies and with different data carriers.
- **Bar code**: Besides providing a legacy resource for migration and integration with RFID, other developments are taking place with the technology including re-writeable bar codes.
- **Real time location**: This technology has some significant overlap in applications with active tag technology.
- **Sensors other than RFID**: Work is taking place on developing standards that integrate sensors with RFID tags. However, in parallel, work is also taking place on other wireless communications with sensors.
- **Emerging technologies**: Various new technologies or components of technologies will have an impact on RFID. Often, such developments take place independently of the standards-making process, but might have a significant long- term impact.
- **Data protection and privacy**: RFID has been seen as the *bête noire* by some campaigners, and virtually singled out as a means of tracking individuals when other long-established technologies probably provide a greater threat (or capability). A key issue is whether enhanced requirements for privacy with RFID will impact on applications.
- **Security**: Until recently, RFID had been considered an enabling technology with low levels of security. Initiatives taken during the GRIFS project have resulted in New Work Items in ISO to define optional security features.

- **Impacting the EU Directives**: There are a number of EU Directives with which RFID must comply. For example, WEEE.

With respect to RFID data processing, we have identified a number of external characteristics that need to be monitored as follows:

- **RFID applications**: As new application areas open up, they will present challenges for processing and integrating the data. An obvious example that is yet to be tested is the implication of sensory data with traceability systems.
- **Bar code applications**: One area that is relatively untested, is the use of bar code and RFID as complementary technologies in the same application.
- **RFID enabling Directives**: Given the EU Commission's interest in promoting the Internet of Things, a number of Recommendations and Directives (e.g. traceability, critical safety) could support the development and take-up of the technology in Europe.
- **Internet of Things**: Here, we are working on the assumption of the Commission's broad concept of multiple classes of object that have associated information accessible via the Internet. As the concept develops into reality, this will impact on RFID data processing.
- **Internet and IETF**: The Internet Engineering Task Force is responsible for all aspects of the Internet, and it is already clear that new approaches will be required to support RFID.
- **Object Naming Schemes**: In addition to finding ways to support extensive legacy data systems, we expect new schemes to emerge for new applications.
- **Network security**: The increased flow of data does require greater network security, particularly given the wireless nature of the air interface.

Figure 2 is a first attempt at identifying crossover influences, and we have no doubts that in the forthcoming years this network of influencing the developments will change.

1.3 Methodology

Once we were appointed to undertake the report, a draft structure was prepared and discussed with the GRIFS project management team. After discussion a format was agreed for the main clause headings that has largely been followed in our subsequent research.

The starting point for the detailed research has been the RFID architecture model that is described in the previous clause. An inventory has been made of standards and/or standardisation developments that specify requirements for a specific part of the RFID architecture model. This approach has enabled us to identify potential overlap or conflict between standards or to identify the need for some new initiatives. Our approach has been firstly to identify these potential areas in terms of topics or issues, and then to identify the stakeholders that are candidates to be members of the Forum.

2 A critical epoch

2.1 The formation of ISO/IEC JTC1 SC31 WG4

The first proposal for the development of a standard in the field of RFID in ISO/IEC JTC 1/SC 31 *Automatic Identification and Data Capture Techniques* was presented on 13 March 1997. The scope of the new work item proposal was 'To define a communication protocol for interoperability of wireless, non-contact omnidirectional radio frequency identification devices capable of receiving, storing, and transmitting data while operating at power levels that are in freely available international frequency bands in the area of item level identification and management across the supply chain such as finished good asset management, raw material asset management, material traceability, inventory control, electronic article surveillance, warranty data, production control/robotics, and facilities management.'

Following the acceptance of this new work item proposal SC31 Working Group 4 (WG4) was created. SC31 WG4 had its first meeting on 26-28 August 1998 in Tokyo, Japan.

2.2 RFID standards and applications before the epoch

Before the formation of SC31 WG4, a number of initiatives to standardise RFID and related technology had taken place. Within ISO itself, the work of JTC1 SC17 on smart card technology was well established and this represented an eventual overlap at 13.56 MHz with the developments in JTC1 SC31 WG4 RFID for Item Management. The United States of America had a number of standards in place under the ANSI / INCITS committee work that were potential candidates for ISO standardisation.

During the course of the GRIFS project, a CEN TC225 Ad Hoc on RFID has been formally changed to a Working Group on RFID. The work undertaken by the group will either be explicitly related to EU Directives, recommendations and mandates, or be used to address applications that have a specific European interest or requirement.

ISO, and other organisations, had undertaken major work developing RFID technology associated with specific applications. These included:

- RFID technology and application standards for animal ID.
- European and ISO standards using RFID for road traffic telematics.
- A set of UPU work-in-progress standards specifying RFID technology at each of the main frequencies.

Apart from the US ANSI standards, there was little previous work on developing standards that only identified the technology and covered a range of RFID frequencies. Most of the candidate technologies were initially considered by WG4 as proprietary, and this resulted in some initial complicated three-stage developments, as will be discussed in 2.4.

Because the technology was proprietary, most of the applications – including some that would eventually migrate to open systems – were for closed systems often limited in scale. These covered a great variety of niche applications – some could be considered to be forerunners of RFID in the supply chain. There were applications for all the main RFID frequencies, with the exception that UHF technology was not used for RFID in many parts of the world because of the potential overlap of that frequency being used for mobile telephones.

2.3 Bar code applications and application standards before the epoch

Bar code and RFID had similar development paths, and were first invented at a similar time in the decade to 1950. The development of bar code, like RFID, was based on proprietary technology, and the companies developing the technology provided solutions for closed system applications.

The major transition for bar code came in the early to mid 1970s. A keynote development was the formation of the Uniform Code Council and then, within a short period of time, EAN International. Other significant organisational developments were taking place in parallel. The manufacturers of bar code technology created their trade association, Automatic Identification Manufacturers (AIM) originally as a product section of the Materials Handling Institute in 1972. The objective was to develop technical solutions, and promote the technology. A significant number of technology exchanges took place, which resulted in previously proprietary bar code symbologies becoming de facto standards. These were finally formalised in 1982 by the publication of a set of symbology specifications. By 1983, AIM had become an independent trade association in the United States, and shortly afterwards progressed internationally with the formation of AIM UK and AIM Europe.

For historical accuracy, we should point out that the Uniform Code Council and EAN International had previously published all the details of their original symbologies.

Developments continued, and members of AIM worked with many different sectors concerned with the development of application standards. Another milestone was the creation of the data dictionary for primary industry originally known as FACT Data Identifiers and later adopted and standardised by ANSI.

By the time of what we have called the "epoch", the formation of SC31 WG4 RFID for Item Management, SC31 WG1, WG2 and WG3 had been in place dealing predominantly with bar code. CEN TC225 had been in existence for some time before this.

The net effect was that by the epoch the bar code vendor community had a deep understanding of application requirements, and the user organisations responsible for developing applications either had significant technical understanding of bar code technology, or could tap into industry resources for this.

Depending on one's perspective and analysis, the progress of RFID was between 12 to 25 years behind what had been achieved with bar code technology by the epoch.

2.4 Early RFID standardisation activities

As previously highlighted, there were some fundamental differences in SC31 with the process to standardise bar code and to standardise RFID. By the time SC31 was created, a number of bar code symbologies (data carriers) had already been published as standards by AIM (which is a formal standards committee of ANSI), by CEN for European standards, and other National Bodies. Therefore, the initial task for bar code was to address the quality of the standard not the technology. Over time, more bar code symbologies were submitted to SC31, but often a significant amount of prior work had been done elsewhere.

In contrast, RFID activities began with almost a blank agenda, although by the time the two RFID Ad Hoc meetings had taken place, there were some clear directions. For a long time, the work of the air interface protocol and the application interface protocol were seen as distinctly separate entities, although there were experts with crossover experience. The brief for the application interface activity was to develop encoding rules that were to be largely independent of air interface issues (as discussed in clauses 7.7 to 7.9).

With the benefit of retrospective analysis, the air interface standardisation activity seems to have progressed through three phases. The first phase was concerned with structuring rules between and within the standards. Whereas each bar code symbology is a distinctly separate data carrier technology standard, an early decision made for RFID was that each part of ISO/IEC 18000 would address a particular frequency. The ideal expressed at the time was to have one air interface protocol per frequency, which was based on a model borrowed from the Universal Postal Union's work on RFID. However, there were many candidate technologies, most of which were effectively proprietary technologies.

The second phase was concerned with the process of reducing nearly 30 candidates into the limited number of standards. For quite some time, there was no consensus on which technology was best in class. So, every time technologies was being evaluated and compared, there were vested interests among other experts, which usually resulted in more informal votes against any given technology than in favour. A key meeting took place in Marseilles, France where all the technology sponsors were offered a straightforward ultimatum. Either face perpetual ballots with the end result of no RFID standards, or work formally or informally together to reduce the variety of candidates. This did lead to a significant amount of collaboration outside the scope of ISO, and enabled the ISO/IEC 18000 standards to move forward and meet the new, more realistic, criteria of up to two air interface protocols per frequency. This position held until stage 3.

At this time, there was still a lot of enthusiasm based on market expectations, and many of the meetings had between 40 to 60 experts participating. It was inevitable that new technology solutions would emerge. Objective criteria that had been applied to bar code standardisation since the formation of SC31 were adapted for RFID. Basically, any new air interface protocol had to be significantly different from those already standardised or carry with it the support of major applications. On this basis, the first serious attempts were made to achieve global acceptance of the UHF frequency with the result of ISO/IEC 18000-6 being developed and published with Type A and B protocols.

The next most significant development, which involved crossover activities between ISO experts, the Auto-ID Labs and eventually EPCglobal, was the process that resulted in the EPCglobal Class 1 Gen 2 (ISO/IEC 18000-6 Type C) air interface. The current position, when the revisions are published, is that:

- four air interface protocols will be included in ISO/IEC 18000-6 (UHF technology): Type A, Type B, Type C, and Type D (previously known as TOTAL).
- three in ISO/IEC 18000-3 (high frequency): Mode 1, Mode 2, and Mode 3

2.5 ISO/IEC JTC1 SC31 WG4

The title of ISO/IEC JTC1 SC31 WG4 is 'RFID for Item Management'. Since its formation, this working group has published 22 standards and technical reports. At this moment 9 of the WG4 documents are being revised and 13 new documents are being developed.

SC31/WG4 now has the following structure:
Subgroup 1 - Application interface protocols
Subgroup 3 - Air Interface
Subgroup 5 - Implementation Guidelines
Subgroup 6 – RFID Performance and Conformance test methods

It has liaisons with the following organisations:

- ISO/IEC JTC1/SC31/WG2 * AIDC – Data Structure
- ISO/IEC JTC1/SC17/WG8 * Identification cards and related devices - integrated circuit cards without contacts
- ISO/IEC JTC 1/SC27
- ISO TC23/SC19/WG3 * Animal Identification
- ISO TC104 * Freight containers
- ISO TC122 * Packaging and JWG * Supply Chain Applications
- ISO/TC184/SC4
- ISO TC204 * Intelligent Transport Systems AIM Global

- CENELEC TC106x * Electromagnetic fields in the human environment
- CEN TC225 * AIDC technologies
- AIM Global
- EDItEUR
- EPCglobal™
- ETSI ERM TG34
- GS1
- IATA
- IEEE
- ITU-R
- Universal Postal Union

2.6 GS1, the Auto-ID Center, EPCglobal

GS1 can trace its antecedents back to 1970, when an Ad Hoc committee of US grocers attempted to agree on the Uniform Grocery Product Identification Code. By 1973, the Universal Product Code symbology had been agreed and is essentially the same symbology used for retail point-of-scanning today. We say essentially the same, because in 1977 the EAN-13 symbology was developed as a natural extension of the UPC code, which extended the capabilities from being a North American product code to being a global code.

Although, over the years, GS1 has focused on fast-moving consumer goods and retail supply chain applications; there are significant other applications that make it the predominant code structure for branded goods. The system does not only focus on the data carrier, but is equally concerned about the data and the communication of data between trading partners. This presented a solid foundation for moving towards a future technology: RFID.

The first initiative with RFID was the development of the GTAG project, which was intended to be a stepwise development from existing RFID technology, building on existing ISO/IEC 18000 standards. This eventually resulted in the publication of the 18000 Type A air interface protocol. A separate development was the creation of the Auto-ID Center at MIT in late 1999, together with leading manufacturing and retailing members of the Uniform Code Council and EAN International. A number of fundamental divisions seem to occur around this time. There was a distinct difference between Europe (leaning towards GTAG), and the US looking for a different approach. The prime technology vendors associated with GTAG were established companies in the RFID community, where those associated with the Auto-ID Center were generally US start-up companies. The first Auto-ID Center specifications (never recognized as EPCglobal standards) were, effectively, a proprietary technology.

Although the GTAG project was due to run and deliver by 2002, it was generally abandoned and all the key players, including many of the traditional RFID vendors, became members of the Auto-ID Center and eventually EPCglobal.

The Auto-ID Center ran in that form to 2003. It developed many concepts, including the principle of a unique code that could be transformed into a look-up system for the Internet. The initial code had no direct relationship to the GS1 code but, eventually, the concept of headers was developed together with the name Electronic Product Code (EPC). At its basic level, this is a serialised version of pre-existing GS1 codes. There are a number of exceptions to the rule in that not all GS1 Global Trade Identification Numbers (whose design was optimised for bar code and certain retail applications) can be converted automatically into an EPC code.

Other codes, such as the GS1 Serial Shipping Container Code were already serialised.

EPCglobal was established on 1st November 2003, with the research side of the Auto-ID Center evolving to a network of University research centres now called Auto-ID Labs and with strong organisation links to the EAN Management Board and the UCC Board of Governors (bear in mind this was pre the creation of GS1). Much of the Work Items that had been addressed by the Auto-ID Center in terms of delivering standards were transferred to EPCglobal, which continues to address the development of standards, often in advance of some of the work in ISO, sometimes in parallel, and occasionally the ISO work moves ahead of specific EPCglobal activities.

3 Stakeholders in the standardisation process

3.1 Introduction

This clause describes the de jure standardisation bodies that develop standards in the field of RFID. Clause 3.2 describes the global standardisation bodies whereas clause 3.3 describes the European standardisation bodies.

3.2 Formal standards bodies at the international level (ISO/IEC, ITU-T)

3.2.1 ISO

ISO is the International Organization for Standardization.

3.2.1.1 Scope

ISO's work programme ranges from standards for traditional activities, such as agriculture and construction, through mechanical engineering, manufacturing and distribution, to transport, medical devices, information and communication technologies, and to standards for good management practice and for services.

3.2.1.2 Membership

Membership of ISO is open to national standards institutes most representative of standardisation in their country (one member in each country).

ISO is made up of 157 members that are divided into three categories:
Member bodies, Correspondent members, Subscriber members.

A member body of ISO is the national body "most representative of standardisation in its country". Only one such body for each country is accepted for membership of ISO. Member bodies are entitled to participate and exercise full voting rights on any technical committee and policy committee of ISO.

A correspondent member is usually an organisation in a country that does not yet have a fully developed national standards activity. Correspondent members do not take an active part in the technical and policy development work, but are entitled to be kept fully informed about the work of interest to them.

Subscriber membership has been established for countries with very small economies. Subscriber members pay reduced membership fees that nevertheless allow them to maintain contact with international standardisation.

3.2.1.3 Deliverables

The following ISO deliverables are available:

Deliverable	Description
ISO Standard	A normative document, developed according to consensus procedures, which has been approved by the ISO membership and P-members of the responsible committee in accordance with Part 1 of the ISO/IEC Directives as a draft International Standard and/or as a final draft International Standard and which has been published by the ISO Central Secretariat.
ISO/PAS Publicly Available Specification	A normative document representing the consensus within a working group.
ISO/TS Technical Specification	A normative document representing the technical consensus within an ISO committee
ISO/TR Technical Report	An informative document containing information of a different kind from that normally published in a normative document.
IWA International Workshop Agreement	An IWA is an ISO document produced through workshop meeting(s) and not through the technical committee process.
ISO Guide	Guides provide guidance to technical committees for the preparation of standards, often on broad fields or topics.

3.2.2 IEC

IEC is the International Electrotechnical Commission (IEC).

3.2.2.1 Scope

The IEC charter embraces all electrotechnologies including electronics, magnetics and electromagnetics, electroacoustics, multimedia, telecommunication, and energy production and distribution, as well as associated general disciplines such as terminology and symbols, electromagnetic compatibility, measurement and performance, dependability, design and development, safety and the environment.

3.2.2.2 Membership

An IEC member is called a National Committee and each NC represents its nation's electrotechnical interests in IEC management and standardisation work.

This includes:
- manufacturers, providers, distributors and vendors
- consumers and users
- all levels of governmental agencies
- professional societies and trade associations
- standards developers

National committees are constituted in different ways. Some are public sector only, some are a combination of public and private sector, and some are private sector only. In this respect, the IEC does not specify how an NC should be formed. It is up to the interested parties in each country to decide how they will constitute their NC.

Kinds of members
There are two forms of active participation in the IEC's work. Full Membership allows countries to participate fully in international standardisation activities. Full Members are National Committees each having equal voting rights. Associate Membership allows for limited participation of countries with limited resources. Associate members may participate in all technical meetings and in the Council and Standardization Management Board meetings held within the framework of the annual General Meeting. They have access rights and can comment on all IEC technical documents (from new work to Final Draft International Standards). In addition, Associate Members may request the IEC General Secretary to become Participating members (P-members) on a maximum of four technical committees and/or subcommittees with the right to vote on technical work emanating from their committees of choice.

Other kind of participation
There is also another kind of participation, spelled out in the Affiliate Country Programme, which is aimed at all newly industrialised countries around the world. It should be noted that Affiliates are neither members nor associate members of the IEC. The Affiliate Country Programme is not a special form of membership.

3.2.2.3 Deliverables

The following IEC deliverables are available:

Deliverable	**Description**
International Standard	A normative document, developed according to consensus procedures, which has been approved by the IEC National Committee members of the responsible committee in accordance with Part 1 of the ISO/IEC Directives as a committee draft for vote and as a final draft International Standard and which has been published by the IEC Central Office.
Technical Specification (TS)	Similar to an IS in that it is normative in nature, developed according to consensus procedures and is approved by two/thirds of the Participating Members of an IEC technical committee or subcommittee. A TS is published when required support for an IS cannot be obtained, or when the subject is still under technical development, or when there is a future - but no immediate - possibility of an IS.
Technical Report (TR)	More descriptive than normative, this is an informative document of a different kind from normative documents (e.g. collection of data). A TR is approved by simple majority of Participating Members of an IEC technical committee or subcommittee.
Guide	Deals with non-normative matters related to international standardisation. An example is the application of "horizontal" standards.

Industry Technical Agreement (ITA)	A normative or informative document that specifies the parameters of a new product or service. It is developed outside the technical structures of the IEC and it helps to enable production and/or market launch of industry products to proceed. It is similar to an industrial de facto standard or specification. Fast moving technology sectors are the main potential users of ITAs, but the whole domain of electrical and electronic engineering (including ICT) may be covered.
Publicly Available Specification (PAS)	A normative document that represents a consensus among experts. A simple majority of the Participating Members of a technical committee or subcommittee approve the document. An IEC-PAS responds to an urgent market need for such a normative document and is designed to bring the work of industry consortia into the realm of the IEC.
Technology Trend Assessment (TTA)	Highlights certain aspects of a technology that might conceivably become an area for standardisation in the near-to-medium term. It responds to the need for global collaboration on standardisation questions during the early stages of technical innovation. A TTA gives the state of the art or trend in emerging fields. It is typically the result of pre-standardisation work or research.

3.2.3 ISO/IEC JTC1

ISO/IEC JTC1 is the Joint Technical Committee 1 of ISO and IEC.

3.2.3.1 Scope

The scope of ISO/IEC JTC1 is standardisation in the field of Information Technology.

Note: Information Technology includes the specification, design and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organisation, storage and retrieval of information.

3.2.3.2 Membership

JTC 1 members are National Bodies. There are 40 Participating (P) Members and 42 Observers (O) Members. Other organisations participate as Liaison Members. There are 14 Liaison members Internal to ISO and IEC, and 22 External Liaison members.

3,2,3,3 Deliverables

The final product of the work conducted within JTC 1 is the published international standard. A JTC1 standard is distinguished by beginning "ISO/IEC" before the number. In addition to this main deliverable, JTC1 develops other standards similar to those developed by ISO.

3.2.4 ITU-T

ITU is the United Nations agency for information and communication technologies. ITU-T is the Telecommunication Standardization Sector.

ITU is based in Geneva, Switzerland, and its membership includes 191 Member States and more than 700 Sector Members and Associates.

3.2.4.1 Scope

The function of ITU-T is to provide global telecommunication standards by studying technical, operating and tariff questions.

3.2.4.2 Membership

Membership of ITU is open to governments, which may join the Union as Member States, as well as to private organisations like carriers, equipment manufacturers, funding bodies, research and development organisations and international and regional telecommunication organisations, which can join ITU as Sector Members.

3.2.4.3 Deliverables

The results of these studies are published as ITU-T Recommendations.

3.3 Formal standards bodies at the European level

3.3.1 CEN

CEN is the European Committee for Standardization.

3.3.1.1 Scope

CEN works in a large number of sectors, in fact in virtually every area that the partner European Standards Organizations, CENELEC and ETSI, do not.

3.3.1.2 Membership

CEN's National Members are the National Standards Organizations of 30 European countries. There is only one member per country. Associate Members are broad-based European organisations, representing particular sectors of industry as well as consumers, environmentalists, workers, and small and medium-sized enterprises.

3.3.1.3 Deliverables

The following CEN deliverables are available:

Deliverable	Description
European Standards (ENs)	In the case of ENs, the Members must transpose the final text ratified by vote into national standards – translating them if desired – but without deviation or alteration, and retain the prefix EN in the national designation: e.g. BS EN 1234, NF EN 1234, DIN EN 1234. Thus the

	number and technical content of the standard are exactly the same throughout Europe.
Technical Specification (CEN TS)	Normative document where the state-of-the-art is not yet stable enough
Technical Report (CEN TR)	For information and transfer of information
CEN Workshop Agreement	For consensual agreements in open workshops

3.3.2 CENELEC

CENELEC is the European Committee for Electrotechnical Standardization.

3.3.2.1 Scope

CENELEC's develops electrotechnical standards.

3.3.2.2 Membership

The 30 current CENELEC members are national organisations entrusted with electrotechnical standardisation, recognised both at National and European level as being able to represent all standardisation interests in their country. Only one organisation per country may be member of CENELEC.

3.3.2.3 Deliverables

The following CENELEC deliverables are available:

Deliverable	**Description**
EN (European Standard)	A normative document available, in principle, in the three official languages of CENELEC (English, French and German) that cannot be in conflict with any other CENELEC standard. EN's are the most important deliverable published by CENELEC. Its development is governed by the principles of consensus, openness and transparency, a national commitment to implement it in each and every one of the member countries of CENELEC, its technical coherence regarding both national and European levels.
HD (Harmonization Document)	Same characteristics as the EN except for the fact that there is no obligation to publish an identical national standard at national level (may be done in different documents/parts), taking into account that the technical content of the HD must be transposed in an equal manner everywhere.

TS (Technical Specification)	A TS is a normative document produced and approved by a Technical Committee (not by CENELEC as such). Several of the compulsory requirements needed to have a standard do not apply to Technical Specifications: there is no standstill, no public enquiry, the vote does not follow the same rules as in the CENELEC Technical Board (where it is weighted). A TS must only be produced in one of the official languages and its maximum lifetime is reduced to two or three years. Technical Specifications are explained in terms of supporting the European Market and act as a guidance method towards evolving technologies and experimental circumstances that would not gather enough consensus as to publishing an EN. A TS may not be in conflict with any other CENELEC standard. If a conflicting standard (EN) is published in the meantime, then the TS must be withdrawn.
TR (Technical Report)	A Technical Report is an informative document on the technical content of standardisation work. Only required in one of the 3 official languages, a TR is approved by the Technical Board or by a Technical Committee by simple majority. No lifetime limit applies.
G (Guides)	CENELEC Guides are informative documents related to the "internal system". They may specify information about standardisation principles and guidance to standards writers. Guides must be approved at General Assembly or Technical Board level. No lifetime limit applies.
CWA (CENELEC Workshop Agreement)	CWAs are an agreement developed and approved by a Workshop through consensus reached among identified individuals and organisations. They must be published at least in one of the official languages. Revision is possible.

3.3.3 ETSI

ETSI is the European Telecommunications Standards Institute.

3.3.3.1 Scope

ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

3.3.3.2 Membership

Membership of ETSI is open to any company or organisation interested in the creation of telecommunications standards and standards in other electronic communications networks and related services.

Various categories of membership are available, depending on the geographical location of the company or organisation and the depth to which it wishes to be involved.

Full membership of ETSI may be obtained by a legal person, be it an association, a company, a grouping, an organisation or a public authority, which is established in a country falling within the geographical area of CEPT and which commits itself to comply with the Statutes and Rules of Procedure of ETSI.

Associate Membership may be obtained by a legal person, be it a company, a grouping, an organisation which is not established in a country falling within the geographical area of CEPT and not eligible for Full membership.

Observer membership may be obtained by a legal person entitled to become a Full or Associate member.

3.3.3.3 Deliverables

The following ETSI deliverables are available:

Deliverable	**Description**
European Standard (or European Norm, EN)	Used when the document is intended to meet needs specific to Europe and requires transposition into national standards, or when the drafting of the document is required under an EC/EFTA Mandate.
ETSI Standard (ES)	Used when the document contains normative requirements and it is necessary to submit the document to the whole ETSI membership for approval.
ETSI Guide (EG)	Used when the document contains guidance on handling of technical standardisation activities, it is submitted to the whole ETSI membership for approval.
ETSI Special Report (SR)	Used for various purposes, including giving public availability to information not produced within a technical committee. ETSI SRs are also used for 'virtual' documents, e.g. documents that are dynamically generated by a query to a database via the web. An SR is published by the technical committee in which it was produced.
ETSI Technical Specification (TS)	Used when the document contains normative requirements and when short time-to-market, validation and maintenance are essential, it is approved by the technical committee that drafted it.
ETSI Technical Report (TR)	Used when the document contains mainly informative elements, it is approved by the technical committee that drafted it.

ETSI Group Specification (GS)	Used by Industry Specification Groups according to the decision-making procedures defined in the group's Terms of Reference. This deliverable type is approved and adopted by the Industry Specification Group that drafted it.

4 The standards making process

4.1 Introduction

This clause describes the standards making process of global and European standards making bodies in the field of RFID.

4.2 ISO

ISO international standards are developed according to the following stages:

Stage, Name and Description	Deliverable	Duration (months)	Deadline (months)
1. Proposal stage The first step in the development of an International Standard is to confirm that a particular International Standard is needed. A new work item proposal (NP) is submitted for vote by the members of the relevant TC or SC to determine the inclusion of the work item in the programme of work.	NP		
2. Preparatory stage A working group of experts, the chairman (convener) of which is the project leader, is set up by the TC/SC for the preparation of a working draft. Successive working drafts may be considered until the working group is satisfied that it has developed the best technical solution to the problem being addressed. At this stage, the draft is forwarded to the working group's parent committee for the consensus-building phase	WD		6 months
3. Committee stage As soon as a first committee draft is available, it is registered by the ISO Central Secretariat. It is distributed for comment and, if required, voting, by the P-members of the TC/SC. Successive committee drafts may be considered until consensus is reached on the technical content. Once consensus has been attained, the text is finalised for submission as a draft International Standard (DIS).	CD		12 months
4. Enquiry stage The draft International Standard (DIS) is circulated to all ISO member bodies by the ISO Central Secretariat for voting and comment within a period of five months. It is approved for submission as a final draft International Standard (FDIS) if a two-thirds majority of the P-members of the TC/SC are in favour and not more than one-quarter of the total number of votes cast are negative. If the approval criteria are not met, the text is returned to the document will again be circulated for voting and comment as a draft International Standard. originating TC/SC for further study and a revised	DIS		24 months

5. Approval stage The final draft International Standard (FDIS) is circulated to all ISO member bodies by the ISO Central Secretariat for a final Yes/No vote within a period of two months. If technical comments are received during this period, they are no longer considered at this stage, but registered for consideration during a future revision of the International Standard. The text is approved as an International Standard if a two-thirds majority of the P-members of the TC/SC is in favour and not more than one-quarter of the total number of votes cast are negative. If these approval criteria are not met, the standard is referred back to the originating TC/SC for reconsideration in light of the technical reasons submitted in support of the negative votes received.	FDIS		33 months
6. Publication stage Once a final draft International Standard has been approved, only minor editorial changes, if and where necessary, are introduced into the final text. The final text is sent to the ISO Central Secretariat that publishes the International Standard.	IS		36 months

4.3 ISO/IEC JTC1

ISO/IEC JTC1 international standards in general follow the same stages as the ISO International Standards.

Stage, Name and Description	**Deliverable**	**Duration (months)**	**Deadline (months)**
1. Proposal stage The first step in the development of an International Standard is to confirm that a particular International Standard is needed. A new work item proposal (NP) is submitted for vote by the members of the relevant TC or SC to determine the inclusion of the work item in the programme of work.	NP		
2. Preparatory stage A working group of experts, the chairman (convener) of which is the project leader, is set up by the TC/SC for the preparation of a working draft. Successive working drafts may be considered until the working group is satisfied that it has developed the best technical solution to the problem being addressed. At this stage, the draft is forwarded to the working group's parent committee for the consensus-building phase.	WD		6 months
3. Committee stage As soon as a first committee draft is available, it is registered by the ISO Central Secretariat. It is distributed for comment and, if required, voting, by the P-members of the TC/SC. Successive committee drafts may be considered until consensus is reached on the technical content. Once consensus has been attained, the text is finalised for submission as a draft International Standard (DIS).	CD		12 months

4. Enquiry stage The draft International Standard (DIS) is circulated to all ISO member bodies by the ISO Central Secretariat for voting and comment within a period of five months. It is approved for submission as a final draft International Standard (FDIS) if a two-thirds majority of the P-members of the TC/SC are in favour and not more than one-quarter of the total number of votes cast are negative. If the approval criteria are not met, the text is returned to the originating TC/SC for further study and a revised document will again be circulated for voting and comment as a draft International Standard.	DIS		24 months
5. Approval stage The final draft International Standard (FDIS) is circulated to all ISO member bodies by the ISO Central Secretariat for a final Yes/No vote within a period of two months. If technical comments are received during this period, they are no longer considered at this stage, but registered for consideration during a future revision of the International Standard. The text is approved as an International Standard if a two-thirds majority of the P-members of the TC/SC is in favour and not more than one-quarter of the total number of votes cast are negative. If these approval criteria are not met, the standard is referred back to the originating TC/SC for reconsideration in light of the technical reasons submitted in support of the negative votes received.	FDIS		30 months
6. Publication stage Once a final draft International Standard has been approved, only minor editorial changes, if and where necessary, are introduced into the final text. The final text is sent to the ISO Central Secretariat that publishes the International Standard.	IS		36 months

4.4 CEN

CEN European standards are developed according to the following stages:

Stage, Name and Description	Deliverable	Duration (months)	Deadline (months)
1. Proposal stage The first step in the development of a European Standard is to confirm that a particular European Standard is needed. A new work item proposal (NWIP) is submitted for vote by the members of the relevant TC to determine the inclusion of the work item in the programme of work.	WI		
2. Preparatory stage The Technical or Project Committee will elaborate a draft standard. In the case of Technical Committees, in order to allow rapid progress in drafting, a smaller group of experts (working group) may be created.	Circulation of first document		6 months
3. Enquiry stage Once the draft is ready a public consultation (enquiry) will take place. This is a key stage in the process of ensuring transparency and acceptability of the standard.	prEN		12 months

4. Approval stage The comments received during the public consultation will then be examined by the TC/PC and the draft will be amended in line with the decisions made by the TC/PC. A report of this process will be carried out and will include justification for comments not taken up. The final draft, once modified, is sent for formal vote. This is a weighted vote of all national standardisation bodies that are member of CEN.			27,5 months
5. Publication stage Once a draft European Standard has been approved, only minor editorial changes, if and where necessary, are introduced into the final text. The final text is sent to the CEN CMC that publishes the International Standard.	EN		36 months

4.5 ITU

ITU standards are developed according to the following stages:

Stage, Name and Description	**Deliverable**	**Duration (months)**	**Deadline (months)**
1. Proposal stage The Question is the basic project unit within ITU-T. Questions address technical studies in a particular area of telecommunication standardisation, and are driven by contributions. Each proposed Question should be formulated in terms of specific task objective(s) and shall be accompanied by appropriate information. This information should clearly justify the reasons for proposing the Question and indicate the degree of urgency, while taking into account the relationship of the work of other study groups and standardisation bodies.	Question		
2. Preparatory stage	Draft Recommendation		
3. Approval stage Once the text of a draft Recommendation is mature, it is submitted for consent at an SG or WP meeting. The consent given by the study group signals the start of the approval process. The mature text will be posted on the ITU-T website. There is then a four-week period in which comments can be made. If no comments are received, the Recommendation is considered approved by the study group chairman in consultation with TSB.	Recommendation	At least 4 months	

4.6 ETSI

ETSI European standards are developed according to the following stages:

Stage, Name and Description	**Deliverable**	**Duration (months)**	**Deadline (months)**

1. Proposal stage The need to create a standard is identified by an ETSI member or group of members, who submit their proposal to the relevant technical committee.	WI		
2. Preparatory stage Once the work item adoption phase is complete, drafting of the standard can begin.		1 to more than 12	
3. Enquiry stage Before a draft EN (telecommunications series) is submitted for ETSI approval a Public Enquiry should have been carried out for this draft by the NSOs.			
4. Approval stage		4 months	
5. Publication stage	EN		36 months

4.7 IEEE

IEEE standards are developed according to the following stages:

Stage, Name and Description	**Deliverable**	**Duration (months)**	**Deadline (months)**
1. Proposal stage A standard begins with a project idea, formally known as a project authorization request (PAR). Upon submission, the PAR is sent to IEEE staff who will review the PAR to ensure the successful submission to the New Standards Committee's (NesCom).	Approved project authorization request (PAR)		
2. Preparatory stage			
3. Enquiry stage A project or draft is ready for a Sponsor Ballot when it has completed its working group (or technical committee) development. After the Sponsor Ballot process is complete, the Sponsor will move the project toward final review by RevCom (the IEEE-SA Standards Board, Standards Review Committee) and approval by the IEEE-SA Standards Board before it is published.			
4. Approval stage Approval of an IEEE standard is achieved by submitting the document and supporting material to the IEEE-SA Standards Board Standards Review Committee (RevCom), which issues a recommendation to the IEEE-SA Standards Board.		Ballots usually last 30 to 60 days.	
5. Publication stage			

4.8 EPCglobal

EPCglobal standards are developed according to the following stages:

Stage, Name and Description	Deliverable	Duration (months)	Deadline (months)
1. Proposal stage The submission track consists of steps designed to ensure that business requirements are captured, validated against the EPCglobal Reference Architecture, and that these requirements for standards are documented. The output of this track feeds into the Standards track. Submission track: Steps 1 and 2: collect business and technical requests/form jrg Step 3: technical definition with users Step 4: end user requirements development Step 5: bsc and tsc approval	Approved Standard Requirements	Up to 10 months	
2. Preparatory stage Step 6: working group formation Step 7: initial standards development	Last Call Working Draft specification	7-8 months[1]	
3. Enquiry stage Step 8: full action group review and approval Step 9: prototype test of candidate specification	Proposed Specification	4 months	
4. Approval stage Step 10: steering committee review	Recommended Specification	1 month	
5. Publication stage Step 11: board of governors ratification	Ratified Standard	1 month	

[1] Can vary, depending on the complexity of the standard

5 The established bar code standards

We have already cited (see 2.3) that bar code standards were well-established even before the creation of SC31. Technology standards were published by CEN/TC 225 and by AIM Global and its affiliated members.

In 1989, one of the authors of this report prepared a document for AIM Europe *Bibliography of Automatic Identification Standards Relevant to Europe* from which we abstract below. The list below identifies known application standards that were in use in Europe in 1989. These include standards from the United States that were adopted by the same sector in Europe.

Organisation	Application Standard	Pub Date
American Blood Commission	Guideline for the Uniform Labeling of Blood and Blood Components	1985
American Paper Institute	Bar Coding Suggested Voluntary Guidelines for Printing-Writing Papers and Newsprint	1983
Automotive Industry Action Group (AIAG)	AIAG-B-3 Shipping/Parts Identification Label Standard	1984
Automotive Industry Action Group (AIAG)	AIAG-B-1 Bar Code Symbology Standard	1984
Automotive Industry Action Group (AIAG)	AIAG-B-4 Individual Part Identification Application Standard	1986
Book Industry Study Group Inc	Machine-Readable Coding Guidelines for the Book Industry	1986
British Office Systems and Stationery Federation	BOSS Federation Guidelines on Bar Code Scanning	1988
British Phonographic Industry (BPI) Ltd	Bar Coding for the Record Industry	1983
Council for Periodical Distributors Associations	Magazine & Paperback Title & Issue Coding UPC Symbol Location and Orientation Guidelines	
Dansk Varekode Administration	PLUS: Price Look Up System	1983
EUGROPA (Union Europeenne des Commerces de Gros En Papiers, Cartons et Emballages)	European Wholesale Paper Merchant Bar Coding Standards	1988
Federation Europeenne des Fabricants de Carton Ondule	Transport Case Symbology Operating Manual	1981
Graphic Communications Association	Specification EMBARC Electronic Manifesting and Bar Coding of Paper Stock Shipments	1985
Greeting Card and Calendar Association	Bar Coding Guidelines for Greeting Cards	1987
Health Industry Bar Code Council (HIBCC)	The Health Industry Bar Code (HIBC) Standards	1985
International Air Transport Association (IATA)	Bar Coding of Baggage Tags – Attachment G: Passenger Services Conference Resolutions Manual	
International Air Transport Association (IATA)	Bar coding of Airlines Tickets – Attachment H: Passenger Services Conference Resolutions Manual	
International Air Transport Association (IATA)	Bar Codes in Cargo Applications – part of Cargo Services Conference Resolutions Manual	
International Article Numbering Association EAN	General EAN Specification	1987
International Article Numbering Association EAN	EAN Coupon Specifications & Guidelines	1987

Organisation	Application Standard	Pub Date
International Federation of Phonogram and Videogram Producers (IFPI)	Recommended Practices for the Uniform Carton Contents Label: User's Guide	1989
Ministry of Defence	Defence Standard 00-34 Standard Symbology for Automatic Identification Marking – Bar Code 39	1986
National Blood Transfusion Service	Specifications for Uniform Labelling of Blood and Blood Products	
Organisation for Data Exchange by Tele Transmission in Europe	ODETTE Transport Label Standard	1986
Periodicals Barcoding Association	Barcoding for Periodicals and Magazines – an Industry Guideline	1985
Publishers Association	Machine Readable Codes for the Book Trade Technical Specification & Operating Manual	1981
Publishers Association	Technical Annexe to MRC Manual Standards for Direct Printing	1986
Recording Industry Association of America Inc	UPC Guidelines for the Recording Industry	1977
Uniform code Council Inc	UPC Film Master Verification Manual	1975
Uniform Code Council Inc	UPD Shipping Container Code and Symbol Specification Manual	1984

For reference, at that time EAN International (now called GS1) had 42 country members, each publishing its own standard based on the General EAN Specifications

6 Established smart card issues

6.1 ISO standards

ISO/IEC JTC1 SC17 *Identification cards* is responsible for developing ISO standards that are associated with smart cards. For this report, we focus only on the standards that have some potential for interoperability and overlap with RFID tags. Therefore, the two prime series of SC17 standards that are relevant are within the responsibility of JTC 1/SC 17/WG 8 *Integrated circuit cards without contacts* are:

- **ISO/IEC 15693 Identification cards -- Contactless integrated circuit cards -- Vicinity cards**
  For all essential purposes, integrated circuits that are compliant with ISO/IEC 15693 are interchangeable with those that claim compliance with ISO/IEC 18000-3 Mode 1. Exactly the same air interface protocol is used. In addition there is a Memorandum of Understanding, fully implemented by JTC1/SC31/WG4, to use a specific set of agreed AFI codes when the devices are used for RFID for Item Management. We are not yet aware that this change has been reflected in the SC17 standards.

- **ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards**
  We understand that there are similarities between the air interface protocol for the ISO/IEC 14443 standards as with ISO/IEC 15693. As the proximity card standards are used as the base set of standards for Near Field Communication, there are significant opportunities, and potential clashes when mobile phones are used to read smart card and RFID tags.

Because of its involvement with Near Field Communication, JTC1/SC6 *Telecommunications and information exchange between systems* has also published standards that have some potential overlap.

6.2 Stakeholders

Three obvious stakeholders are the three JTC1 sub-committees: SC6, SC17 and SC31. The potential overlap at 13.56 MHz is a prime target for detailed Memorandum of Understanding between these three committees - who have some degree of formal liaison status – but have very little levels of activity taking place between them.

ECMA International
European Committee for Banking Standards (ECBS)
International Air Transport Association (IATA)
International Card Manufacturers Association (ICMA)
International Civil Aviation Organization (ICAO)
United Nations Economic Commission for Europe (UNECE)

From the financial sector, the following commercial organisations: American Express, MasterCard International, and Visa International

6.3 Issues with current and future RFID technology

The potential overlap between smart card and RFID has been significantly under-estimated, without too much consideration being given to potential benefits and problems. The focus of the two relevant ISO committees is on applications: SC17 on **Identification cards**, SC31 WG4 on **RFID for item management**. But aspects of the technology overlap in the standards domain and in products. One application area where the overlap is understood is with RFID for libraries. Fairly basic (ISO/IEC

18000-3 Mode 1) RFID tags are used on the loan items, but the patron cards are compliant with ISO/IEC 15693, and often include vendor-specific additional security features. This is because such patron cards often are not exclusively used by the library, but are used for other services provided by the library owner, whether it is a local government authority or a university.

While this is an example of a reasonably well-managed interface, we are not aware of responsible actions being taken to avoid 18000-3 Mode 1 tags (intended for RFID) not being used for smart card environment and smart cards not being used in an RFID environment.

The situation becomes more complex given two future developments. The first is promulgation of Near Field Communication data capture, which not only enables a mobile phone to be an RFID/smart card reader, but also allows the phone to emulate tag functionality. In addition, if the mobile phone is capable of writing data, then data on 18000-3 Mode 1 tags could be changed. Further research is required to establish the capability not only of the standards, but also with device upgrades.

The other development is the introduction of ISO/IEC 18000-3 Mode 3 (EPCglobal HF Gen 2) RFID tags. As these are intended to be interoperable with 18000-3 Mode 1 tags, a number of overlapping features need to be taken into account.

7 Classification of RFID and related standards and regulations

7.1 Frequency regulations

7.1.1 Overview

The frequency regulations govern specific aspects of radio spectrum and permitted power for an RFID system or other radio communication system. Therefore, radio regulations – as they are commonly called – have a direct and indirect impact on the use of RFID technology. Some regulations apply specifically to RFID, and others apply to any radio device operating with a particular part of the radio spectrum. The radio regulations impact the way an RFID air interface protocol may be implemented. Because the structure for managing the radio spectrum is on a national and regional basis, radio regulations impose constraints on the way RFID may be implemented within a particular national or regional geographic domain.

7.1.2 Key relationships with other components of an RFID system

The radio regulations have a direct relationship with each air interface protocol as shown in Figure 3 and have an implied "normative reference". Because of the potential difference in regulations in different parts of the world, specific radio regulations are not quoted in these terms in the RFID standards. Instead, air interface standards generally indicate that a system "shall comply with local radio regulations".

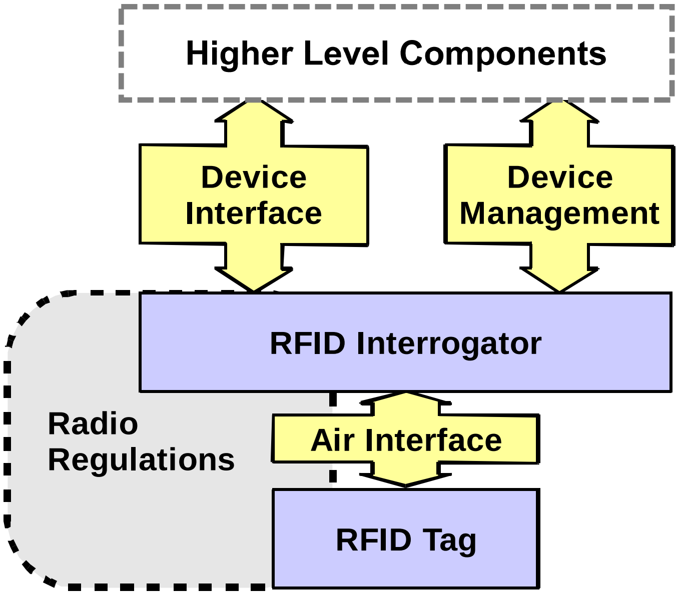


Figure 3: The Radio Regulations in relation to other system components

7.1.3 The European regulations

We mentioned earlier that there is a regional basis for harmonising radio regulations. In fact, ITU-R has attempted to sub-divide the world into three regions: the Americas, Europe and Africa, Asia and Australasia. The reality is somewhat different, because there are significant national variations in each of these regions. This covers: generic spectrum management issues independent of types of device, then specific regulation for types of device such as RFID with specific bandwidths at which communications may take place, with the size and number of communication channels, and the power that may be applied.

Europe is an interestingly different situation. CEPT, the European Conference of Postal and Telecommunications Administrations, is tasked by the European Commission with a basic aim to strengthen the relationship between the 46 members of CEPT to promote co-operation and to contribute to the creation of a dynamic market in the field of European posts and communications. The 46 members include all EU member states as well as all acceding, candidate and EEA countries.

Whereas CEPT is co-ordinating the 46 administrations, it has a Memorandum of Understanding with ETSI that is assigned the responsibility of delivering the appropriate standards.

The prime ETSI standards, technical reports and technical specifications associated with radio regulations for RFID are:

- ETSI EN 300 220
- ETSI EN 300 330
- ETSI EN 300 440
- ETSI EN 302 208
- ETSI TR 102 436
- ETSI TS 102 562
- ETSI TR 102 649

Some of these standards are two-part standards, and some have also been updated by revisions.

The GRIFS RFID Standards Database (http://grifs-project.eu/db/) provides greater details of each of these standards, together with the associated EC Decisions and Directives.

7.1.4 Significant development areas

One of the biggest challenges as RFID air interface protocols (see 7.4) were being developed was to achieve some form of harmonisation of the radio regulations. This was to ensure that an RFID tag could be applied and encoded in one country and be readable in a number of other countries. Because of the nature of source marking items with RFID tags, there is often no certainty in which countries an item will appear in its lifetime.

A reasonable degree of harmonisation of regulations had been achieved at some frequencies, particularly 13.56 MHz whereas, however, Europe allows higher power levels than the rest of the world. One of the significant problems was achieving harmonisation within the UHF spectrum. In fact, some major countries involved with the development of the ISO RFID air interface protocols (particularly Japan and Korea) were obliged to vote initially negatively for ISO/IEC 18000-6 as it progressed because radio regulators in those countries did not permit **any use of RFID** within that spectrum.

A key driver to achieve some form of harmonisation was the development of the EPCglobal standards. Being the RFID equivalent of the GS1 standards, the EPCglobal standards have the prospect of being implemented on a global basis. Countries such as the United States, where UHF has been permitted for some time were able to show that UHF technology had a proven track record of providing the performance requirements in supply chain situations. Various actions were required to achieve global acceptance of RFID in the UHF spectrum, including some form of harmonisation in Europe and persuasion of the radio regulators in countries such as Japan and Korea to permit some part of the UHF spectrum for the use of RFID.

However, to achieve this required a high degree of compromise and also acceptance of some progressive steps in moving forward. Whereas the United States could operate RFID system frequencies between 902 MHz and 928 MHz, other countries had no spectrum available equivalent to that bandwidth or even within part of that spectrum. In fact after all the processes to achieve some form of solution to enable global RFID applications, the air interface protocol standards have been specified to function between 860 MHz and 960 MHz. In addition, many regulators only allowed a very small bandwidth, which restricted the number of channels that can be used in a reading system, which affects the performance capability in terms of the number of tags that can be read in a given period of time.

Even though the situation is far from ideal, at least the current position is that RFID UHF systems can be used in most parts of the world. The situation of harmonising International regulation still remains a problem although, but over the medium term, some of the differences are expected to disappear or reduce.

As part of the ongoing work to increase awareness of the differences and encourage the reduction of the impact of differences in radio regulations for RFID technology, a sponsored database is maintained by AIM Global. It contains over 1500 relevant regulations. We are also aware that a specific work package to address radio regulations is part of the CASAGRAS project. As a result, this GRIFS report only focuses on European standards.

A lot of progress has been achieved in the adoption of adequate regulations for using RFID at UHF. As of the end of 2008, the countries having proper regulations in place represent more than 98% of the world's gross national income. See report on Regulations at
http://www.epcglobalinc.org/tech/freq_reg/

7.2 Health and Safety regulations

7.2.1 Overview

There are two primary Health and Safety aspects associated with the use of RFID:

- The effect of electromagnetic waves consisting of both a thermal effect (a warming effect on body tissue) and the non-thermal effect. These are covered by exposure limits defined in standards and regulations discussed below.
- The other issue is concerned with potential interference between RFID devices and implanted electronic medical devices.

7.2.2 Key relationships with other components of an RFID system

Logically, both these Health and Safety requirements need to be incorporated into the RFID air interface conformance standards. This is certainly a position that has been recognised by JTC1 SC31 – at least in principle. The real challenge is that conformance standards are focused exclusively on air interface conformance, and the impact on the human body in terms of a SAR value (Specific Energy Absorption Rate) depends very much on the design and manufacture of an interrogator. Therefore, this calls for type testing of devices rather than just a mention in the generic air interface conformance standard.

There are two additional features that also need to be taken into account. The International guidelines defined by ICNIRP (International Commission on Non-ionising Radiation Protection) specify significantly different SAR values for employees (on the assumption that training and supervision of the use of equipment is in place) as distinct from the significantly lower levels of exposure to the general public. Equipment therefore might be suitable for use in the industrial or commercial environment, but not to the general public.

The second point is that from independent research carried out by the authors, we are aware that some vendors confuse these specific requirements of human exposure to be more general EMC requirements. In fact, we have seen details of a major vendor self-certifying against the EMC requirements and claiming that these applied to the thermal effects of electromagnetic waves.

7.2.3 Significant development areas

The initial guidelines were published by ICNIRP in 1998 and were followed quickly by a European Council Recommendation (1999/519/EC). In turn, this led to the CENELEC standard mentioned below, and ultimately the International standards.

Whilst there is reasonable acceptance by some medical practitioners of the thermal effect of electromagnetic waves on the human body, a major problem still exists with respect to potential interference between RFID devices and implanted electronic medical devices. Generally speaking, such medical devices are designed and tested against a set of likely devices that might interfere, but as new technology such as RFID is introduced and enhanced, implanted devices cannot be expected to have in-built features that deal with non-interference. From discussions during the ISO committee meetings with the regulators and manufacturers of such medical devices, it is clear that the onus of non-interference is expected to rest with the manufacturers of RFID devices. To this extent, again the ISO committee of JTC1 SC31 WG4 has taken an initiative to ensure that there is "…self-certification that RFID emissions and susceptibility comply with IEC 60601-1-2."

7.2.4 Regulations and standards

Further details of the ICNIRP guidelines and the Commission Recommendations are provided on the GRIFS RFID Standards Database:
http://grifs-project.eu/db/

This database also includes further details of the CENELEC standards that have been in place for some time:

- CLC EN 50364
- CLC EN 50357

It also includes details of IEC standards that are in place or under development.

7.3 Data protection and privacy regulations

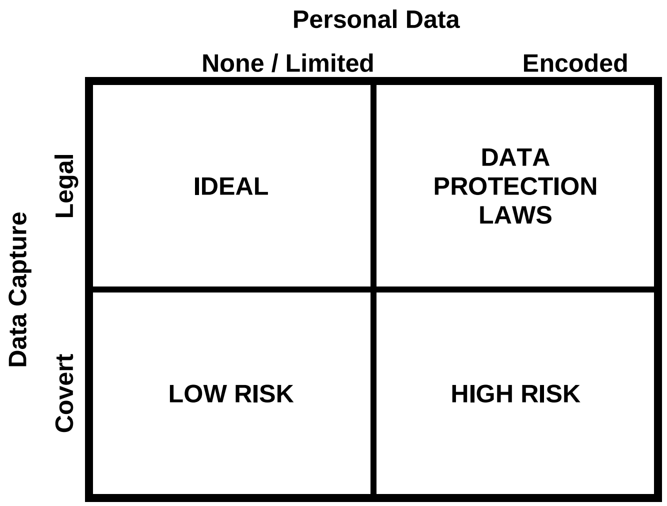
7.3.1 Overview

There is significant confusion among the general public – and even legislators – about data held on an RFID tag and the ability to track individual people using the air interface protocol.

The current legal position in Europe is that any personal data held on an RFID tag or associated with an RFID tag is subject to the Data Protection Directive (2002/58/EC). This applies to the direct naming of an individual, or a code on the tag that can directly be associated with the individual and linked through a database to that individual. As such, this aspect of data protection is identical whether the data is encoded on an RFID tag or in a bar code.

The privacy concerns are generally focused on the ability to use RFID technology to read without a line of sight. Sometimes, the stated performance capabilities – in terms of read range and tag singulation – are grossly exaggerated compared with normal performance capabilities. Some of the claimed reading ranges require emitted power that is illegal under the radio regulations. Therefore, some of those concerned with privacy scares associated with RFID seem to accept that breaking the laws associated with radio regulations combined with covert surveillance will become the norm.

We consider that any balanced discussion on data protection linked to RFID data capture should take into consideration the following simple matrix Figure 4.



		Personal Data	
		None / Limited	Encoded
Data Capture	Legal	IDEAL	DATA PROTECTION LAWS
	Covert	LOW RISK	HIGH RISK

Figure 4: Risk Matrix

The matrix attempts to discriminate between encoded data and data capture. If no personal data is encoded and data capture is only in legal applications the reality of risk is zero. At the other extreme, the inclusion of personal data combined with whatever real level of covert data capture leads to a strong perception that there are risks from RFID technology. These points are discussed below.

Hitherto, standards work on data protection and privacy has been limited. Following an overview report from a CEN/ISSS Focus Group, a CEN Workshop has existed for some years, however this has mainly prepared CWAs concerning how businesses generally can meet legal requirements (e.g. by protecting customer and client data). One current work item however concerns a technology watch system as to how to ensure that technological developments meet the legal requirements – clearly this should include RFID also.

7.3.2 Key relationships with other components of an RFID system

There are two separate relationships (discussed below). One is between data protection and the tag architecture and air interface protocol; the other is with the data content.

7.3.2.1 Tag architecture and air interface

There have been a number of proposals, particularly from an academic base, to introduce privacy enhancing techniques (PETs) to RFID technology. Few, almost none, of such PETs are so far present in the devices and the air interface protocol standards.

This gives rise to how it is possible to introduce such PETs by retro-engineering into existing technology, for example for any given air interface in the ISO/IEC 18000 series of standards. Various considerations need to be considered:

- Cognisance has to be taken of the infrastructure of readers and tags that are in place.

- In addition, this infrastructure will continue to grow using existing technology (i.e. without the PET) until the standard is in place and products implemented – a period of at least three years.
- Adding new features to an existing standardised technology is difficult to achieve as a mandatory requirement, so a general rule of thumb is that additional features are added as optional features.
- Given the above, it is impossible to make assumptions about the voluntary take-up of any new feature.

To achieve some form of full compliance, some legislature would have to mandate that a specific PET is incorporated in RFID tags for particular applications. That legislature would then have to take into account the political implications and commercial implications for its business stakeholders:

- International trade has to be taken into account, particularly the fact that when tags are applied at source, often the ultimate market is unknown.
- It is likely that a tag with additional features, particular to support some PET function, will be more expensive than any prevailing tag.
- In addition, there is already an ongoing drive to embed RFID tags within products, or to integrate tags at early stages of production. Some PET proposed solutions will require some re-tooling of production processes, processes that will themselves be relatively new and not achieved their return on investment.
- Even if the tag technology is changed, the reader infrastructure might not be able to be upgraded to support any new PET functionality.
- Additionally, any given legislative authority will need to persuade others states for all tags from a given date to comply with PET as a mandated component.

In reality, citizens of most countries in the world carry smart cards, which have a significantly higher potential of carrying personal data or with directly associated codes to personal data than an RFID tag used in supply chains. At some frequencies, the performance of a smart card and an RFID tag is exactly the same and use exactly the same air interface protocols. The threat that is cited as "new" with the introduction of RFID has, in fact, existed for more than a decade with minimum concern. In addition to smart cards, technology such as mobile phones, Bluetooth, and near field communication have, or will, pose the same threats – possibly more so than RFID, but none of these technologies are perceived as a bête noire as is RFID technology.

7.3.2.2 Data content

It is far easier, and probably more effective, to impose constraints on what data may be encoded in an RFID tag. To comply with the data protection requirements, the basic advice that should be adopted by any application standard is to encode the minimum, or no, personal data. Most RFID technology will be associated with item-related data and not personal data, in sharp contrast to the smart card. For most applications, there is little need for any form of personal data to be encoded on the RFID tag.

An additional consideration is association of data on the RFID tag, for example, through a retail database to the individual customer. Linking products to customers has been possible in practical terms since 1973 when bar code scanning was adopted in the retail sector. It existed probably 10 to 15 years earlier than this with OCR data capture in the retail sector.

A major difference with RFID is the capability or requirement for serialisation, so that each tag is uniquely distinguishable from other tags. This gives rise, and some justification to the claim that that the RFID tag can be associated with a specific individual. There are three general ways that serialisation is achieved:

- A number of air interface protocols require a unique tag (really a chip) identifier. This is used by the anti-collision algorithm to select one tag from others that may be in the reading field to enable communication with that tag and no others. In addition, this chip ID can make a positive contribution to some applications because it can contribute systems where product authentication is a requirement.

- The EPCglobal system requires the use of a serial number not for anti-collision requirements (because other approaches are used) but for traceability in the entire system. This uniqueness is applied locally, and may be retained on records maintained by the company responsible for invoking the data capture procedure. However, being able to trace information that has an association with that serial number (for example through the Object Name Service) is not possible because the ONS system does not require the serial number to be used for resolution purposes and any access to a specific serial number requires additional levels of permissions.

- Other serial numbers exist, and for illustration we will use the IATA Baggage Identification Number. Within the secure air transport systems, there is obviously a direct association between the baggage identification number and the passenger, or at least the passenger's family. By the way, this has been the case since baggage identification systems using bar code were introduced in the mid-1980s. A key point here is that there is no public access to resolving the Baggage Identification Number; such data is held on secure systems. In fact, access to the data is restricted to the encoding airline or airport with access provided on a "needs basis" to other airlines and airports within the sector. Similar restrictions apply in other sectors, not just to protect the privacy of the individual citizen, but also to protect commercially sensitive data.

In addition to fundamental permissions to access data, anyone wanting to identify an individual reading a chip ID on an EPCglobal code, or on an IATA baggage tag identifier would need to access the correct database. No specific database is retained of chip IDs used purely for anti-collision purposes. It might be possible to identify an airline or other air transportation entity with part of the code on the Baggage Identification Number, but the location of the particular computer-based database would still remain unknown, except to someone inside the industry, and then only to someone with access to the particular database.

Although it is theoretically possible for anyone to access the ONS on the basic product identification, most general enquiries from citizens will probably only return details such as the product description. In other words, without levels of permission - that are part of the database security not the RFID technology itself - access to personal data from RFID tags can be difficult, or made to be difficult by invoking basic data protection principles and processes.

7.3.3 Documents

The GRIFS RFID Standards Database (see http://grifs-project.eu/db/) includes further details of the CENELEC standards. It also includes source information for the following:

- European Data Protection Directive
- The Canadian Guidelines on the use of RFID
- The Washington State, USA law making it illegal to capture data from RFID tags for illegal purposes
- The draft ISO standard on the RFID emblem

7.3.4 Significant development areas

As soon as the prospect of RFID technology became a serious possibility, some lobbyists in developed economies started to treat the technology as "spy chips". As part of the response to this, various legislatures began to address RFID in privacy as a specific topic and as something different from other technologies associated with data capture linked to requirements of data protection.

An early example of a balanced view came in guidelines for RFID in libraries developed by the Information & Privacy Commissioner of the Province of Ontario in Canada. The Ontario guidelines

(Guidelines for Using RFID Tags in Ontario Public Libraries) draw a distinction between RFID technology and smart card, where a completely different guideline is in existence.

The library guidelines were followed up in 2007 with a more generic document entitled *Privacy Guidelines for RFID Information Systems* listing three over-arching principles, abstracting directly from the document:

1. **Focus on RFID information systems not technology**: The problem does not lie with RFID technologies themselves, it is the way in which they are deployed that raises privacy concerns. For this reason, we prefer to speak broadly of RFID *Information Systems*.
2. **Privacy and security must be built in from the outset** – at the design stage.
3. **Maximal individual participation and consent**.

It is interesting that this document – in just four pages – presents an extremely balanced view of privacy and RFID.

The Commission of the European Union has been working on a Recommendation on RFID privacy, data protection and security. The COMMISSION RECOMMENDATION of 12.5.2009 *on the implementation of privacy and data protection principles in applications supported by radio-frequency identification* was published earlier this year. The Recommendation includes the following:

- that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments
- that operators
    - ❑ conduct an assessment of the implications of the application implementation for the protection of personal data and privacy
    - ❑ take appropriate technical and organisational measures to ensure the protection of personal data and privacy
    - ❑ make available the assessment to the competent authority at least six weeks before the deployment of the application
    - ❑ develop and publish a concise, accurate and easy to understand information policy for each of their applications
    - ❑ take steps to inform individuals of the presence of readers on the basis of a common European sign

The last point above is explicitly repeated for RFID applications in the retail sector. Then there are additional complexities that require some evaluation and judgement. While there is no requirement that tags placed on or embedded in product should carry an additional signal, there is still a requirement to assess whether such tags in operations where there are no RFID applications pose threats to privacy or the protection of personal data. There is also a basic requirement to deactivate or remove the point-of-sale tags that are part of an RFID application – but this obviously cannot be invoked in a retail operation that carries tagged products but has no RFID device to deactivate the tag. However, even for those retailers that implement RFID data capture, if the privacy and data protection impact assessment concludes that the tags place no threat to privacy or protection of personal data after the point-of-sale, the retailer has no requirement to deactivate all the tags, but still needs to provide the customer with an easy means of achieving this.

There is no doubt that PETs will be developed and will be implemented in RFID technology. There is a close relationship between privacy and security. A new Work Group has been created in JTC1 SC31 to deal explicitly with security and its first work items are concerned with adding security features to RFID tags in the ISO/IEC 18000 series. It will still be two to three years before the standard and associated products are on the market. But the Commission is expecting a full response to the Recommendation from member states before this essential standards work is completed. There is a risk that a new EU Directive might not align with internationally standardised technology. From a standardisation perspective, such changes need to be implemented in a formal and open manner and not dependent upon proprietary technology. Using any proprietary technology for items that can be sold by different retailers will only result in a fragmented solution.

A serious problem is that the existing RFID technology is being implemented on a daily basis, increasing the size and value of the infrastructure and providing inertia to any form of switch-over. The scale of the problem is not unlike changing railway track gauges, changing roads and vehicles so that all countries drive on the same side (other than the political inertia). A closer reference of technology inertia can be made with reference to the fact that retail bar code scanning is using a 35 year old technology that has not been significantly upgraded despite lots of opportunities to introduce technical advances, it certainly has not been replaced, and RFID is the first new technology to be proposed to operate in parallel. New bar code symbologies (data carriers) are being introduced, but usually with a 5 to 7 year phased introduction.

If PETs are introduced as options in the RFID technologies, then requirements for their use might be specified for particular applications. In these circumstances take-up can be accelerated. However, applying them to general item level coding for retail products is an extremely difficult challenge to implement, even within the European Union, given the global trade implications.

An interesting development took place in Washington State, USA last year, where a new law was brought in to make "skimming" (the unauthorised reading of data stored on an RFID tag) for criminal purposes such as fraud, identity theft or stalking, a Class 3 felony subject to up to 5 years imprisonment and a $10,000 fine. This is considerably more severe to a parallel development in California (yet to be enacted as law) where the punishment level is approximately 20% of those of Washington State. What is interesting about these developments, is that the focus is on the covert and illegal reading of RFID tags, which has been much of the concern of the responsible consumer lobbyists across Europe. By introducing a law that clarifies illegal actions, the covert access to RFID described in the matrix diagram above, now makes it a criminal offence to capture data for the particular illegal activities cited by the Washington law which became effective July 2008.

Recent analysis suggests that up to 20 states in America have enacted or are considering legislation to regulate RFID in some capacity. The legal system in the United States embodied in the philosophy of "Congress versus the States" could lead to a fragmentation of laws. So, to some extent, the European Commission Recommendation applying to 27 member states might, at first sight, appear to be better. One of the key elements missing from the Recommendation is a focus on defining legislation that makes certain acts such as those defined in Washington State as "skimming" to be criminal offences.

As part of the approach to advise consumers of the presence of RFID, proposals have been put forward for symbols or emblems to be installed where RFID systems are implemented, and even on packages containing RFID tags. There is even an ISO standard, currently work-in-progress, for such an *RFID Emblem*. There are some significant issues that need to be taken into account prior to reaching the conclusion that this is a "good idea". Not all countries see the need for such an emblem for privacy purposes. In fact, the concern in Japan is more to advise that an RFID system is implemented, rather than an RFID tag is present, so that citizens with implanted electronic medical devices are aware of the need to take appropriate precautions. Some of the considerations include:

- The cost of providing an "RFID inside" type of emblem will increase the cost of packaging, and if predictions of a large-scale take-up are justified, RFID would be ubiquitous just as is the EAN/UPC-A bar code on retail products.
- An RFID emblem on product packaging provides no indication of the existence of an RFID data capture in a particular retail store, adding to the confusion of consumers.
- Whereas the ISO standard is based on a proposal from AIM Global, there have already been negative comments from National Standards bodies. In addition, we are aware that other emblems are being considered; for example there is currently a competition taking place in Germany for the design of such a symbol. The realistic outcome is that there will be a number of different "competing" emblems and, with International trade, consumers are likely to be more confused than enlightened.

7.4 Air interface standards

7.4.1 Overview

The air interface standard primarily affects the components of the RFID system: the interrogator and the tag by defining rules for communication between the two devices. In particular, an air interface standard specifies:

- Detailed protocol rules, including modulation and bit encoding so that communication rules that are relevant to the air interface can be distinguished from any other radio signal, including noise.
- The anti-collision algorithm that is used to singulate an individual tag from others to maintain an open communication channel.
- Structures for commands and responses, including the specification of additional processes required when invoking commands.
- Some aspects of memory architecture, including the definition of specific memory areas for particular functions, size constraints on particular memories, whether and how this memory is locked.

7.4.2 Key relationships with other components of an RFID system

Apart from the air interface between the interrogator and the RFID tag, the interrogator also communicates with the layers of the application through the device interface and device management systems (see 7.7), as illustrated in Figure 5. This type of systems architecture usually applies to medium and large size network systems.

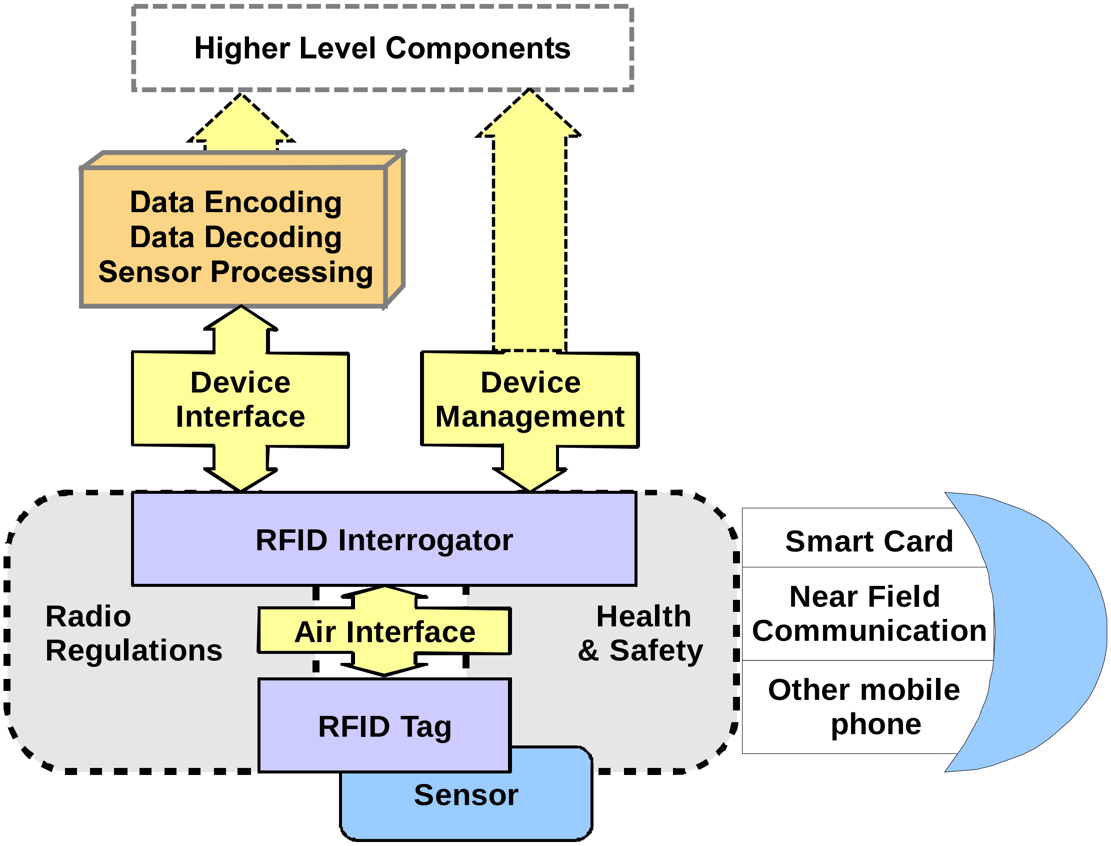


Figure 5: The air interface as part of a larger system

RFID can obviously support simpler systems, even with one interrogator, and here the interface with the interrogator is often through some proprietary or XML interface defined by the device manufacturer. Increasingly, printer-encoder devices are supporting an XML interface, enabling simpler integration with any type of application.

Figure 5 illustrates an RFID system, but there are three other types of air interface or linked communication that are discussed elsewhere in this report:

- At 13.56 MHz, the RFID air interface protocol known as ISO/IEC 18000-3 Mode 1 is also used as the air interface for smart cards. The advantage of this is that it allows some degree of integration and data carriers to identify individuals (with smart cards) can be linked with data carriers to identify items (with RFID). There are some complex issues such as keeping the standards aligned for some characteristics and allowing some degree of independence between the two applications.
- The situation with respect to smart card has become more complicated by the fact that the smart card standard ISO/IEC 14443 has also been adopted for use by the Near Field Communication Forum. The relevant documents are defined as "tag specifications" and there are likely to be overlapping issues as the technology is developed (see more detailed discussions in clause 9.7).
- In recent years, increased efforts have been made to link sensors to RFID tags in a standardised manner, and this work will soon result in published standards. The sensor has no direct means of communication with the application but is required to do this using one of the RFID air interface protocols (see clause 7.7 for a more detailed discussion).

7.4.3 Standards

The main air interface protocols are used for identifying items from the ISO/IEC 18000 series of standards (see the GRIFS RFID Standards Database, http://grifs-project.eu/db/ for details) are:

- ISO/IEC 18000-1 – Reference architecture and parameter definition
- ISO/IEC 18000-2 – Parameters at <135 kHz
- ISO/IEC 18000-3 – Parameters at 13.56 MHz
- ISO/IEC 18000-4 – Parameters at 2.45 GHz
- ISO/IEC 18000-6 – Parameters at 860 to 960 MHz
- ISO/IEC 18000-7 – Parameters at 433 MHz

Most of these standards were originally published in 2004, but continued enhancements have meant that revisions are in progress to add new features to specific air interface protocols, sometimes to add new air interface protocols at a given frequency.

The EPCglobal standards are also included in the GRIFS RFID Standards Database, but are essentially identical to specific ISO standards shown in Table 1.

Frequency	ISO	EPCglobal
13.56 MHz	ISO/IEC 18000-3 Mode 3	HF Generation 2 Tag Protocol
	Status: work-in-progress	Status: not yet published
860 – 960 MHz	ISO/IEC 18000-6 [Type C] Amendment 1	Class 1 Generation 2 UHF Air Interface v 1.1.0
	Status: published	Status: superseded (see below)
860 – 960 MHz	ISO/IEC 18000-6 [Type C] Revision 1	Class 1 Generation 2 UHF Air Interface v 1.2.0
	Status: work-in-progress	Status: work-in-progress

Table 1: Relationship between ISO and EPCglobal standards

7.4.4 Significant development areas

As shown above, the main developments of air interface protocol standards take place within the JTC1 SC31 committee or EPCglobal. EPCglobal has taken the lead in the development of its standards, which are then presented to ISO for additional review and potential developments.

The process of ongoing developments is likely to continue for a number of years, even given the ISO selection criteria that a new technology needs to provide features that are not addressed in existing standards. As an example, the following is an analysis of the work-in-progress that has a direct impact on ISO/IEC 18000 standards:

- ISO/IEC 18000-6 Type C is undergoing enhancements to align with EPCglobal's next version, but additionally to support simple and full function sensors and battery-assisted communication.
- A new air interface protocol Type D is being introduced in ISO/IEC 18000-6. Previously known as TOTAL (tag-only-talks-after-listening) this air protocol can deliver its entire payload as soon as it has harvested the field energy. TOTAL is being specified to support simple sensors.
- A new Mode 3, as detailed above, is being introduced in ISO/IEC 18000-3.
- New proposals for a work item on security issues is likely to require additional features to be added to air interface protocols.

In addition to the ISO criteria that new RFID air interface technology needs to provide different, or enhanced, features, each new development needs to be interoperable or backwards compatible with what already exists at the given frequency. For example, 18000-6 Type D requires the *after listening* feature to ensure that implementations of this air interface protocol does not interfere with existing 18000-6 features. The addition of the variety of features to 18000-6 has required a significant amount of engineering to ensure that products already in the market are not compromised by the inclusion of the new features in new tags and readers.

The current position with 18000-6 Type C and EPCglobal Class 1 Gen 2 developments is that this is an area that requires more technical integration. The current indications are that 18000-6C will include support for features such as battery-assisted communication, full function sensors and simple sensors, whereas these might not appear in the next EPCglobal standard. The simple fact is that the investment required to develop and bring to market specific RFID chips means that too much divergence between the standards of these organisations can be a serious impediment to the take-up of the technology. In the past, there have been instances of potential divergence that have been resolved, but ongoing developments need to be addressed to avoid duplication and contradictions.

Interoperability between air interface protocols has become more complex, given the developments of adding RFID functionality to mobile telephones (see 9.7 for a more detailed discussion). In essence, developments are taking place to use mobile phones either at 13.56 MHz or in the UHF band of 860 to 960 MHz. If the mobile phone retains a basic function of being a reader, then it is like any other interrogator. However, some of the developments include using the mobile phone as a tag emulator, where the extent of the functionality needs to be clearly understood by stakeholders in the different standards-making application areas.

7.5 Sensor standards

7.5.1 Overview

Often the term "sensor" is used in an imprecise and ambiguous manner. At one extreme this term includes RFID tags that only encode data; another accepts sensors correctly as being within the class of transducers and actuators but ignores significant differences in the means of communication from the sensor to the application and the topology of a sensor network. This report adopts a specific approach to the question of "what is a sensor?" Firstly, a sensor monitors and reports on an environmental characteristic that affects the item to which it is attached; it does not contain item-related data. Secondly, it is important to distinguish the means of communication between the sensor to the application. In this report the means of communication is restricted to an RFID air interface or a similar interface mechanism from an RTLS device. In other words, the sensor is an embedded or physically connected "peripheral" of the RFID tag or RTLS device.

For an RFID-sensor tag, the air interface is that of the RFID component, with additional RFID air interface commands required to support sensor functions such as reading sensor data and configuring the sensor. The sensor commands and responses are transported over the air interface from the RFID interrogator to the RFID tag and internally transferred to the logic associated with the sensor for processing. The method of connecting sensors to RFID tags is usually considered beyond the scope of standardisation.

7.5.2 Key relationships with other components of an RFID system

The work that has so far been done to develop standards for sensors for RFID has focussed on two fundamental classes of sensor:

- Simple sensors where the minimum of data is transferred in a small data packet, typically 32 bits to 48 bits, which not only provide summary environmental data, but also limit the types of sensor and their measurement range.
- Full function sensors that – in principle at least – support the monitoring of any physical characteristic, and reporting this over any feasible range of values for that characteristic.

The interface between the sensor and the RFID tag is via some physical channel such as a serial communication port, or by incorporating all or some of the sensor functions on the same integrated circuit as the RFID tag. Because of this it is possible to have a set of common sensor commands that are independent of the air interface, but for these to be embedded in transport commands that are compliant with the air interface. These points are illustrated in Figure 6.

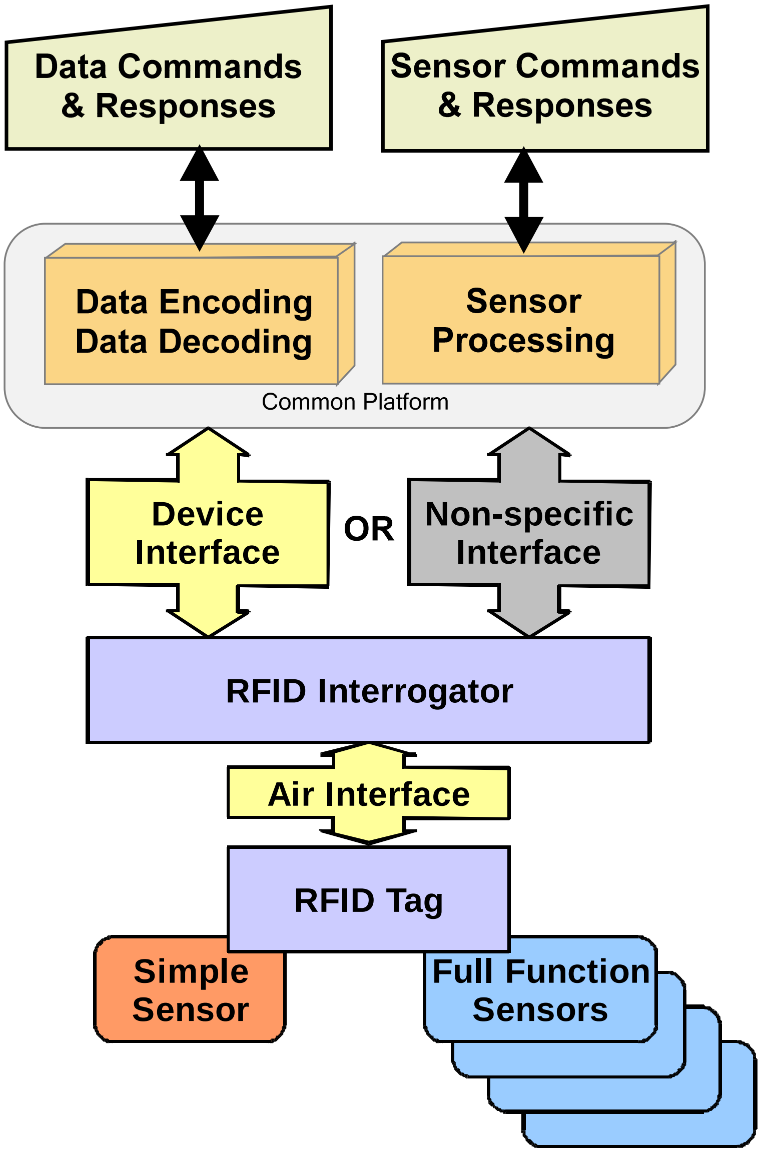


Figure 6: Sensors in relationship to other system components

Within this system architecture, the interrogator can provide different levels of sophistication, ranging from the interrogator passing the raw sensor output data (contained in responses to commands) to a higher level processor, to an interrogator that has integral support for all the processes. The means of transfer can be achieved by using one of the device interface standards (see 7.7), or using some other type of interface, ranging from proprietary to generic (e.g. XML). Interpretation for full function and simple sensors is carried out to the rules of ISO/IEC 24753.

7.5.3 Standards

The standards that specify sensors are:

- IEEE 1451.7 for full function sensors
- ISO/IEC 18000-6 for simple sensors
- ISO/IEC 24753 for the processing of sensor data from both types of sensor.

Details are provided in the GRIFS RFID Standards Database (http://grifs-project.eu/db/).

The RFID air interface standards that currently have provisions to support sensors are ISO/IEC 18000 Parts 6 Type C and Type D. Although it had been expected that ISO/IEC 18000-7 would have been revised to support sensors in a standardised manner, the sponsors of this technology did not provide enough technical input to the relevant committees. It is also expected that RTLS standards (see 7.14) will support sensors.

7.5.4 Significant development areas

Many technical issues have been addressed during the development of the various sensor and sensor-related standards. This has resulted in a clear distinction between the two classes of sensor. Because of the prescriptive measurement capability of simple sensors and they way that their essential data can be delivered, each RFID tag can only support one simple sensor. In contrast a number of full function sensors (each monitoring one physical feature, potentially covering any SI unit (Systeme Internationale d'Unities, commonly known as the metric system) or derived SI unit: temperature, humidity, shock) may be supported by a single RFID tag. In turn, each sensor may be capable of delivering different types of measurement: e.g. peak value, average, a data log of out-of-range values.

There is now the potential to move sensory data capture from a base of proprietary technology and closed system applications, to one of standardised technology and open system applications. Support can be added to interrogators that support the air interface protocols that already specify support for sensors, and to other air interfaces in time.

One of the air interfaces, ISO/IEC 18000-6C, is equivalent to the EPCglobal Class 1 Generation 2 RFID air interface. EPCglobal has yet to undertake its own development work for sensors, and it would be unfortunate if different solutions were developed for the same interface.

With technology standards in place, opportunities will present themselves to use sensors in different applications, particularly for traceability of items that are sensitive to environmental factors, such as perishable foods, vaccines, and items subject to physical damage by being mishandled. RFID sensor-tags can also be placed in fixed locations that need to be monitored regularly.

In future there can be significant developments for applications using sensors should the European Union decide to use the technology in support of existing directives or to establish new requirements. Prime targets are in the field of public health associated with the monitoring of some foods from source to consumer and of temperature sensitive pharmaceutical products.

7.6 Conformance and performance standards

7.6.1 Overview

There are two primary types of standard within this category:

- Conformance standards specifying how to test individual features of an air interface protocol standard, and they can be applied selectively to the functions implemented on the interrogator or on the tag.
- Performance standards that are of a generic nature to enable a manufacturer to make explicit claims about performance. Within this group, there are sub-sets that might apply to specific types of device.

In addition, these standards may be used in test procedures so that products may be certified for use in particular situations. This is certainly an activity that has been undertaken by EPCglobal, and is discussed in more detail below.

There are other types of conformance standards and certification procedures that are discussed elsewhere in this report.

7.6.2 Key relationships with other components of an RFID system

The conformance and performance standards are directly associated with specific air interface protocol standards. They simply define test procedures for the features of the air interface standards.

7.6.3 Standards

7.6.3.1 ISO standards

The ISO standards are sub-divided into three series:

- ISO/IEC 18046 for RFID performance standards.
- ISO/IEC 18047 for RFID conformance standards at specific frequencies.
- ISO/IEC 24769 and 24770 for RTLS Device Conformance Test Methods

Details are included in the GRIFS RFID Standards Database (http://grifs-project.eu/db/).

7.6.3.2 EPCglobal standards

The EPCglobal standards currently only address the UHF Class 1 Gen 2 air interface protocol. Because of this, the types of standard are slightly different from those of ISO as follows:

- The conformance standards only address the EPCglobal equivalent of ISO/IEC 18000-6C.
- The performance standards are addressed specifically at the tag and at particular types of reader. In contrast, the ISO standards are more generic.
- In addition, EPCglobal specifies interoperability test requirements.

The GRIFS RFID Standards Database (http://grifs-project.eu/db/) identifies, in more detail, the relevant standards.

7.6.3.3 EPCglobal Certification

EPCglobal has operated a certification programme for UHF Class 1 Gen 2 devices. There are two levels of certification:

- Products can be certified as compliant with the conformance standards.
- Products that are certified as interoperable have first to satisfy the basic conformance requirements and are tested against other system components that are compliance certified. As a result, products that are Interoperability certified provide the user community with the confidence that various types of component devices from different manufacturers are possible to integrate in one system.

The types of device that are certified under either scheme are all EPCglobal UHF Class 1 Gen 2 devices, including:

- Tags and integrated circuits (the RFID chip).
- Readers and reader modules.
- Printers that are capable of encoding RFID tags.

Figure 7 illustrates the two EPCglobal certification marks that appear on devices and on product literature.

Figure 7: EPCglobal Certifiction Mark

The url for the list of certified products is: http://www.epcglobalinc.org/certification/hw_cert/

7.6.4 Significant development areas

Each time a new air interface protocol is standardised, there should be a requirement for a new conformance standard and possibly for a performance standard. To date, the development of conformance and performance standards always lags behind the availability of the air interface technology standard. At one level, this fits in with a traditional cycle where only prototyping is done during the development of the standard, so no real products are available until after publication.

However, one of the trends in the development of air interface protocol standards is for some of the technology development to take place in parallel – despite the risks of subsequent deviation from the published standard. So there is an earlier marketplace requirement for conformance standards. In fact, there is every justification for working on the conformance standards in parallel or with no more than the slightest time lag.

With the development of technologies similar to RFID – such as RTLS – there is an increasing trend within the JTC1 SC31 committee for conformance issues no longer to be seen as generic, but to need to reside significantly closer to the Work Group developing the technology standards. In 2008, the JTC1 SC31 WG3 SG1 RFID conformance committee was disbanded, effectively removing its direct association with WG3 Conformance, and re-assigned as a sub-group (SG6) of SC31 WG4 RFID for Item Management. Parallel to this, conformance projects for RTLS technology have been transferred to SC31 WG5. Since then, as WG3 Conformance was only focussed on optical data carriers, its work has merged with JTC1 SC31 WG1 Data Carriers.

Recently, the JTC1 SC31 WG3 SG1 RFID conformance committee was disbanded, effectively removing its direct association with WG3 Conformance (which is now more focussed on optical data carriers), and re-assigned as a sub-group (SG6) of SC31 WG4 RFID for Item Management. Parallel to this, conformance projects for RTLS technology have been transferred to SC31 WG5.

EPCglobal's development of a product certification programme is interesting. We observe that at a similar stage in its development (probably in the period 1976 to 1980), GS1 did not adopt any form of device certification programme. So, the development of the certification programme is both novel in its concept and to be applauded for the benefit of that particular user community.

Similar certification programmes could be developed for other sectors, using the EPCglobal as a general model but with necessary differences. There are other applications (baggage handling and automotive as examples) using the same air interface protocol that might not be able to depend on the EPCglobal certification. This is because differences in the amount of data encoded on the RFID tag and the type of data capture would certainly require additional work to be undertaken for such applications within the relevant user community. In fact, only in recent weeks has IATA identified five ISO/IEC 18000-6C tags that meet its requirements for baggage handling.

If the application called for an air interface protocol other than 18000-6 Type C, then additional layers of consideration would need to be taken into account. The US Department of Defense has conducted interoperability trials for devices whose manufacturers claimed compliance with the ISO/IEC 18000-7 standard. Although this is a well-established technology, until a recent assignment of licences to a number of organisations, this was effectively a *de facto* proprietary technology. The licensing of the technology has increased the need for interoperability between devices.

Both the EPC and DoD initiatives suggest that developing some kind of certification programme is desirable and possible in the early days of the deployment of the technology. A bigger challenge exists with a long-established technology such as the 18000-3 Mode 1 air interface protocol where, because of its link with smart card, there is a rough estimate of over 1 million readers already deployed. However, even with this technology as true open system application standards are developed (e.g. in this particular case ISO 28560 for RFID for libraries) then interoperability becomes an issue if users are to gain all the benefits of open systems. We understand that with the increasing use of ISO/IEC 18000-3 Mode 1 tags in the library community (at a recent library conference it was stated that there are 2500 RFID-enabled libraries worldwide) that the vendor community in Germany has started to develop some interoperability test procedures. The UK organisation Book Industry Communications in its e4libraries initiative is introducing accreditation for RFID library systems.

7.7 Device interface standards

7.7.1 Overview

The device interface standards and the data application interface protocol standard (see 7.8) are closely related. The distinction that we draw in our structure is that the device interface standards deal predominantly with the networking of RFID devices, whereas the application interface standard – even those using the same standards – deal with the processing of data read from an RFID tag or written to an RFID tag.

We draw this distinction because for long-established RFID technologies the device interface mechanisms are generally proprietary, but these air interfaces can still use some of the application interface protocol standards.

The genesis for standardisation can be traced to the development by EPCglobal for its low-level reader protocol standard, which currently only applies to the EPCglobal UHF Class 1 Gen 2 air interface (equivalent to ISO/IEC 18000-6C). ISO did not start work on the software system infrastructure (the ISO/IEC 24791 series) until after this initial work by EPCglobal. The scope of the ISO work is intended to be wider, with the prospects of supporting any of the ISO/IEC 18000 air interface protocols.

7.7.2 Key relationships with other components of an RFID system

Two classes of standard comprise the device interface:

- The device interface standards themselves, which have a dual function. They provide instructions to the interrogator, transfer data between the application and the interrogator in a format that the interrogator can convert into air interface commands.
- Device management standards that relate to the initialisation, monitoring, and control of RFID devices in a networked environment.

Because there are security aspects associated with the communication between devices, these also need to be taken into account. Figure 8 shows the relationship between the device interface and management standard with other components.

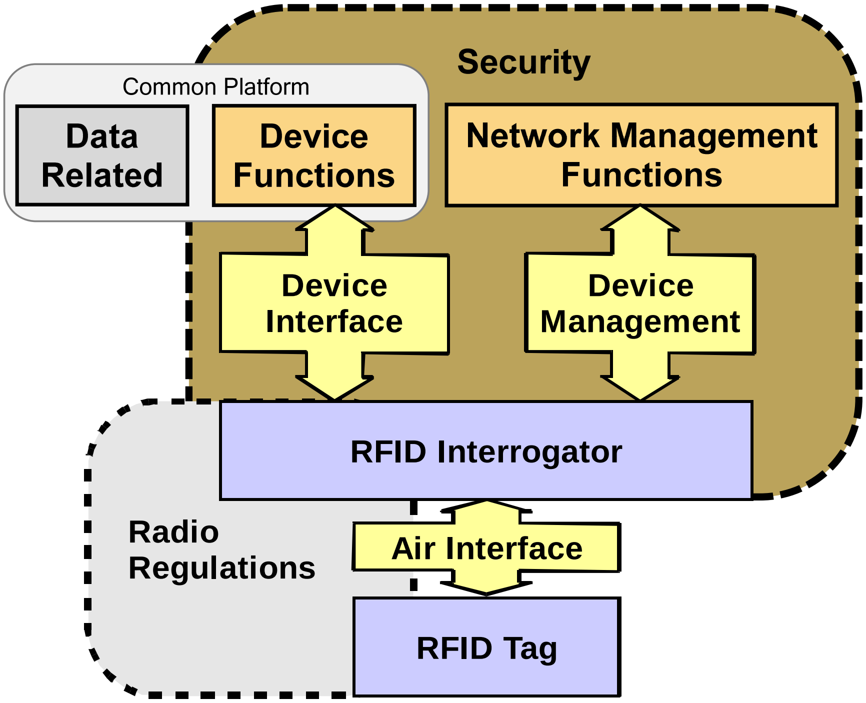


Figure 8: Device interface & management standards: Interrelationships

It should be noted that the figure includes the radio regulations, because these need to be taken into account in the way that devices are configured to operate in a legal context within the different regulatory authorities.

Currently, the device interface standards are fairly limited in scope, with the ISO standards only addressing ISO/IEC 18000-6C (in a similar way that the EPCglobal standards only address UHF Class 1 Gen 2).

The data management standards are still in an embryonic state, as discussed below.

7.7.3 Standards

7.7.3.1 ISO standards

There are two standards that are relevant to this area of the RFID system, with the first two being of primary relevance and the security standard having an indirect impact. The standards are:

- ISO/IEC 24791-5 Device Interface
- ISO/IEC 24791-3 Data Management

NOTE: ISO/IEC 24791-6 has since been withdrawn so that all security work can be undertaken in the new committee: ISO/IEC JTC1 SC31 WG7 Security

Further details are provided in the GRIFS RFID Standards Database (http://grifs-project.eu/db/), which also lists ISO/IEC 24791-1 that defines the overall architecture of the software system infrastructure.

7.7.3.2 EPCglobal standards

EPCglobal has three standards in this area of development:

- The low-level reader protocol standard, which is similar to the ISO device interface standard and focuses on 18000-6C technology.
- The reader management standard, which has parallel with the ISO device management standard.
- Discovery, configuration and initialisation standard for reader operations (which is still in development) and whose functions are also embodied in the ISO device management standard.

The GRIFS RFID Standards Database (http://grifs-project.eu/db/) describes these standards in greater detail.

7.7.4 Significant development areas

For the discussions about developments, it probably makes sense to discuss separately issues concerned with the device interface standard and device management standard.

7.7.4.1 Device interface

The function of the device interface has always been necessary and, traditionally, has been provided as a proprietary solution by individual reader manufacturers. This is not something that is unique to RFID, and has been fairly common with bar code devices for some considerable time. Traditionally, the only way around the challenge of trying to communicate with a "different" AIDC device has been through the use of emulators developed by various device manufacturers. These allow components of their systems to talk to devices from other manufacturers.

EPCglobal took the view in developing its Low Level Reader Protocol (LLRP) standard that having a common interface, which supported all the standardised features for an interrogator, would be a "good thing" and still allow product innovation for interrogators and the higher level software. To achieve this, some fairly basic level of communication was agreed upon and all the messages in the LLRP standard, and also in ISO/IEC 24791-5 are simple binary-structured messages. The only difference between the EPCglobal and the ISO standards is that ISO needs to support additional messages because of ISO's support for more complex data. The development of such standards could only take place because of the fact that the infrastructure for interrogators for ISO/IEC 18000-6 Type C was relatively small and immature compared with that for other air interfaces. Therefore, the investment in developing this type of standard would only be justified at this stage of deployment of the technology. Prime targets for new device interface standards should include ISO air interface protocols that are still at an early stage of deployment.

The real challenge exists in whether it is possible to develop such standards retrospectively for long-established air interface protocols operating in other frequencies. One method that can be considered is to take a different approach, and not necessarily standardise the interface, but "expose" interfaces with the components that would otherwise sit at either end of a device interface standard. There have already been developments in this direction, particularly from RFID printer encoder manufacturers. In addition to supporting their proprietary encoding language and protocols, some provide an additional interface by exposing XML interfaces. If a software application above the interrogator is also XML-enabled, then it is possible to develop specific interfaces between the components. Although this is not necessarily as "standardised" as a device interface standard, it certainly improves the opportunity for cross-collaboration in a manner that is significantly simpler than having to address the detailed proprietary interrogator programming language and protocol.

7.7.4.2 Device management

There are commercially available proprietary device management systems, but the work undertaken by EPCglobal and ISO is reasonably innovative. It seems that basic device management is not the challenge. The real challenge is how to address this in a network. This is being addressed by the EPCglobal Discovery, Configuration and Initialisation (DCI) standard. The DCI approach enables readers and access controllers to "discover" one another. In addition, they enable identification and authentication to take place before committing to ongoing communication.

The EPCglobal DCI standard is in turn based on the IETF Control and Provisioning of Wireless Access Points (CAPWAP) standard, which is itself still undergoing development work.

The committee developing ISO/IEC 24791-3 has taken these developments into consideration. In addition to building the ISO standard on the EPCglobal approach, another factor has been introduced. This is to use Web Services to provide an XML means of communication for device management.

The process is also challenging for EPCglobal because the intention was to complete the DCI standard in early 2008, but the IETF work is still ongoing as this report is published.

7.8 Data encoding and protocol standards (often called middleware)

7.8.1 Overview

The data encoding and protocol standards address the various types of communication between the RFID interrogator and the application, with the exception of not dealing with the device interface and device management functions (see 7.7).

7.8.2 Key relationships with other components

Figure 9 shows the relationship of this type of standard with the application layer and the RFID interrogator.

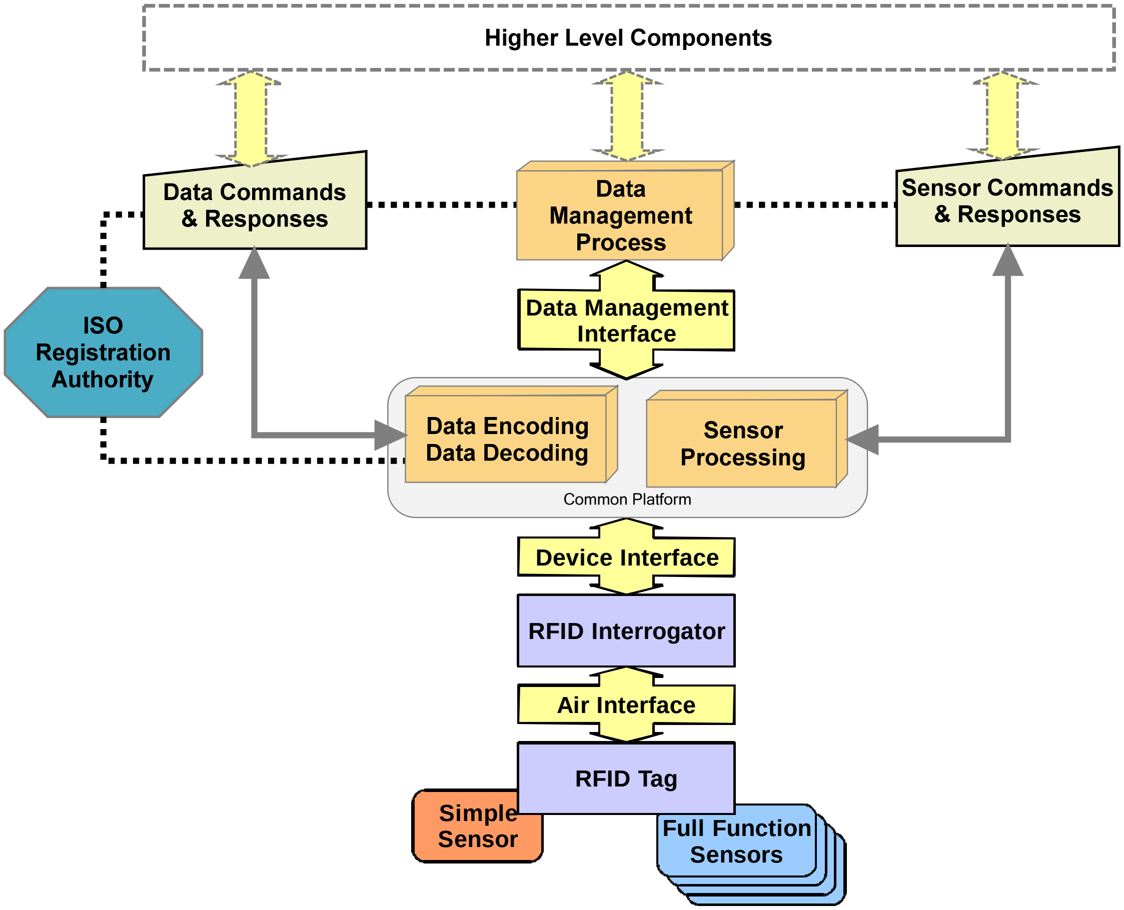


Figure 9: Data encoding and application protocol standards: interrelationships

The device interface provides a common message structure to communicate encoded bytes to and from the interrogator. This component has a dual role for transporting data and data-related commands and configuration instructions to the interrogator (as discussed in 7.7).

The data encoding process converts application-based data (as is displayed on a computer screen) into more efficiently compacted string of bits or bytes for encoding on the RFID tag. Included in this process is additional formatting to take into account features such as the tag architecture, selective locking of memory on the RFID tag, and any metadata required to be encoded on the RFID tag. In parallel to this is the processing of sensor data (as discussed in 7.5). Because sensor data needs to relate to the environment to which some physical object had been exposed, there is a high probability that there will be a link in processing object-related data and sensor data.

The data management interface defines the message structures for communicating between the application layer and the data management processes. The processes themselves are not subject to standardisation, allowing for different types of product to be developed and deployed in applications.

The vertical flow through the middle of the Figure 9 identifies components that are part of a networked system. There are two other implementation issues that need to be considered, The command / response components represent standalone processes that have been designed, and in the case of object-related data implemented, as a direct method to address aspects of data management through explicit functional commands and responses. The dotted line relationship between these components and the data management processor is to indicate that to produce compliant encoding, sensor configuration, and correct interpretation that these functional rules need to be addressed.

Also shown on the figure, and an essential component for the ISO standards and applications is a Registration Authority that assigns and registers codes (known as data constructs) to enable different applications to use the same air interface protocol and other components in a fully inter-operable manner.

7.8.3 Standards

7.8.3.1 ISO standards

The relevant ISO standards are:

- The ISO/IEC 15961 series for commands, responses and application related data
- ISO/IEC 15962 for data encoding and decoding
- ISO/IEC 24791-2 for data management
- ISO/IEC 24791-5 for relevant aspects of device interface (see also 7.7)

See the GRIFS RFID Standards Database (http://grifs-project.eu/db/) for details.

7.8.3.2 EPCglobal standards

The relevant EPCglobal standards are:

- Low Level Reader Protocol (LLRP) for relevant aspects of device interface (see also 7.7)
- Application Level Events (ALE)

See the GRIFS RFID Standards Database (http://grifs-project.eu/db/) for details.

7.8.4 Significant development areas

The work of JTC1 SC31 WG4 SG1 was probably the first standardisation attempt to produce generic encoding rules for RFID technology. The encoding rules of ISO/IEC 15962 are generally independent of the application, taking application data and encoding this in a standardised manner in a similar way to that used for bar code symbologies. The difference with bar code encoding rules is that the RFID encoding rules are largely independent of the particular tag architecture and air interface protocols. This is achieved through a logical mechanism known as a tag driver. The encoding rules support encoding of a single data element, or multiple data elements, on an RFID tag.

The EPCglobal standard started with a significantly simpler data encoding rule, focusing on various structures of the EPC code. However, in contrast to the ISO work, EPCglobal undertook a significant amount of pioneering work in developing the interface standards that are essential between the interrogator and the application for networked systems. Until this work was undertaken, users depended on proprietary solutions; and this still applies for systems based on long established air interface protocols. The prime EPCglobal standards are the Application Level Events (ALE) specification and the Low-Level Reader Protocol (LLRP) standard.

The significance of the EPC work for a device interface standard is such that some of the ISO/IEC 24791 standards (see above) are closely modelled on these standards. The ISO standards are intended to provide additional functionality for the types of RFID tag and application not directly relevant to EPCglobal.

Currently, the complex data encoding that the ISO Standard is required to address is not yet supported by the EPC standards. Certainly, a significant number of use cases have been put forward to EPC over recent years that require data in addition to the basic EPC serialised code. This additional data will require some form of complex coding, and the EPCglobal standards are likely to be published with this type of support in due course.

The structure defined in Figure 9 is still being slowly adopted by different industries, with the majority of the focus being on data encoding and decoding. This essential component is not appreciated by many organisations responsible for designing application standards. Furthermore, there are still major sectors that are totally unaware of the standardisation efforts.

The Registration Authority is receiving a number of enquiries from organisations in different sectors, but many of these organisations do not understand all of the issues involved. Promoting the benefits of the standards and the function of the Registration Authority seems to be beyond any organisation's remit.

The situation is probably indicative of an even greater misunderstanding about RFID among those responsible for developing application standards. So far, some applications to the Registration Authority indicate that some organisations are unaware of the different air interface protocols, that RFID communications are different from bar codes, and that it is possible to selectively read and write and modify data. The implication of this is that there are assumptions that bar code encoding rules can simply be applied. Because user organisations generally interface with vendors, who are not necessarily aware of all the standards issues, there can be a significant gap between the users' understanding and the reality.

7.9 Data standards

7.9.1 Overview

The data standards address the way data is held in business applications. As such, they are associated with the data dictionaries developed by user organisations for encoding in various AIDC data carriers. In some cases, the legacy requirements of encoding in bar code need to be taken into account with encoding in RFID; in other cases, slightly new approaches can be adopted.

For the purpose of this report, we cannot explore all the different types of data that are defined by different application standards. We concentrate on a few of the primary codes, particularly those adopted on a widespread basis and applied generically across sectors.

We also discuss a challenge that exists when integrating RFID with pre-existing bar code technology, because bar code data capture, whether from a single linear symbol or a complex 2D symbol, is an all-or-nothing capture technique. Encoding rules that apply to those technologies might not be the most appropriate ones for RFID with the capability of selective reading and writing and modifying and deleting data selectively. This has an impact on the relationships, as discussed below.

7.9.2 Key relationships with other components

In order to understand the relationship with other RFID components, consideration needs to be given to three classes of data standard:

- **Unique Item Identifiers** which, irrespective of the data carrier technologies, are able to identify uniquely an item within the domain and scope of an application. We make this qualification about domain (or namespace) and scope because there are many false assumptions that any one scheme is the one that provides uniqueness, and that uniqueness is assumed to be a timeless parameter.

- **Data dictionary standards** that define individual data elements, which have specific meaning within application domains.

- **Message standards**, particularly with respect to their role of identifying primary data dictionaries.

Figure 10 shows the relationship with these standards and predominantly the data encoding and decoding processes that then link down to the data encoded on the RFID tag.

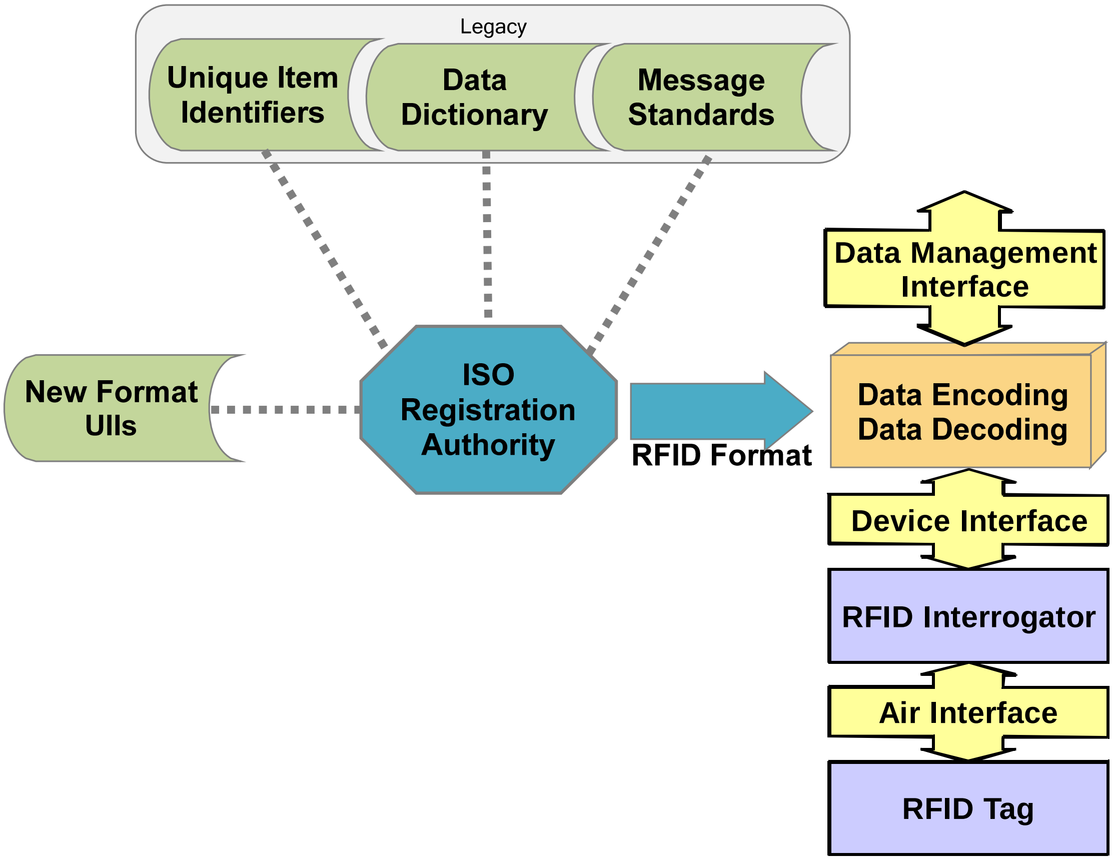


Figure 10: Data standards: interrelationships

The figure shows that the Registration Authority is fairly key to this process. Although the flow appears to be through the Registration Authority, it is actually using code structure registered with the Registration Authority to achieve data presentable in an RFID format.

To be compliant with ISO standards, the RFID format needs to be based on object identifiers, which ensures uniqueness from the business application through to the tag. The use of object identifiers in RFID applies to all the legacy types of data, including the unique item identifier.

It even applies to new classes of unique item identifiers. There is one exception to this rule, which is the set of serialised EPCglobal codes. These codes can be encoded directly on the RFID tag, but this approach carries a penalty. By being the exception to the rule only tags that have specific architectural structures can support the EPCglobal code structure without it being linked to an object identifier structure.

An interesting future challenge is how EPCglobal addresses the encoding of object-related data such as batch number and expiry date, which are strongly supported along with many other data elements by the well-established GS1 Application Identifier dictionary.

7.9.3 Standards

7.9.3.1 ISO standards

The relevant ISO standards are:

- **The ISO/IEC 15459 series of standards for unique identifiers**. Object identifier structures are defined within these standards for the ISO/IEC 15459 identifiers that can be unique to the individual data carrier. Other codes, for example batch numbers, can obviously be defined as unique data, but have to be treated as attribute codes within an RFID tag to avoid the risk of two tags having such a code as a unique identifier.
- **ISO/IEC 15418** which, in turn, points to the two major data dictionaries used in bar code applications. These are the GS1 Application Identifiers and the ANSI MH10 Data Identifiers. Each of these schemes already has a defined method for converting into an object identifier structure for encoding in an RFID tag and for the RFID communication chain.
- **ISO/IEC 15434**, which defines a message structure which is highly suitable for a "read all" type of data capture environment. Some of the types of messages are themselves based on data dictionaries, which are potential candidates for being registered with the Registration Authority for RFID data constructs. The syntax of ISO/IEC 15434 does present challenges for direct encoding in an RFID tag in as much as it is encoded and decoded as a single object, which ignores the selective read and write capabilities of the technology and the air interface transition issues.

See the GRIFS RFID Standards Database (http://grifs-project.eu/db/) for details.

7.9.3.2 EPCglobal standards

The relevant EPCglobal standard is the EPC Tag Data Standard (TDS). The current published version only specifies the serialised codes, i.e. those that are unique identifiers.

See the GRIFS RFID Standards Database (http://grifs-project.eu/db/) for details.

7.9.4 Significant development areas

One of the early challenges for JTC1 SC31 was how to identify data in a structured manner that would be invisible to the human eye. This was necessary to ensure that only tags that belonged to a specific domain were read. Other data would need to be ignored and excluded from the domain at the earliest possibility. None of this was possible with the closed systems applications for RFID, and data could be transferred from the interrogator to the application and only then identified as not being part of a domain. There was always the statistical risk that some false data would be ambiguous and be accepted.

By adopting an object identifier structure, every individual piece of data encoded on an RFID tag can be identified and arranged in whatever logical sequence made sense. The rules for object identifiers are specified in ISO/IEC 9834-1 and, by their very nature, object identifiers can be extremely long. The advantage they offer of being applicable to any type of data, including the extensive legacy data already supported by bar code technology, had to be balanced by some efficient means of encoding on the RFID tag.

Discussions with the relevant ISO committee resulted in a new structure for an object identifier, basically partitioning it into two parts:

- A Root-OID, that identifies all the common arcs of the object identifiers encoded on the RFID tag.
- A significantly shorter Relative-OID for the remaining part of the object identifier, with only this part encoded on the RFID tag.

The Root-OID can be implied, but to ensure interoperability of standards, part of the work of the Registration Authority is to assign a Data Format that is encoded on the tag and declares the Root-OID. This approach enables efficient encoding on the RFID tag, but all the communications from the device interface upwards can be based on the full object identifier to avoid any ambiguity within the systems.

The reason that object identifiers were selected as this mechanism, was because they are already well-established and used to identify network devices and any data. There is an interesting circular relationship between object identifiers and uniform resource names, as used on the Internet. The OID structure is a proper sub-set of the URN system but, in turn, the URN is a proper sub-set of the object identifier system. What matters is the context. So, it is possible to encode a URN on an RFID tag using an object identifier structure. It is also possible to resolve an object identifier over the Internet.

In addition to supporting legacy data systems, and the EPCglobal serialised codes (which themselves are derived from the GS1 legacy data systems) RFID brings with it an opportunity and requirement for new types of unique item identifiers. These include code structures such as an IPv4 or an IPv6 Internet address, the Japanese Ubiquitous Code, and others that may emerge in the future.

One of the challenges of encoding legacy data is that this is sometimes long and structured with punctuation and other characters for ease of reading by humans. There are two reasons why this presents a problem for RFID:

- The first, and most serious, one is that a number of tags have a limited encoding capacity (particularly for the UII) and many of the legacy codes are too long to be encoded.
- Even if a tag has the capability of encoding a long legacy code, this still requires more air interface transmission time and if the requirement is to read multiple tags quickly, this can also present a problem. For example, as a forklift truck is unloading a pallet of items from a delivery vehicle at a receiving bay, each item might need to be read. High-speed conveyor systems present another problem and, for example, the IATA baggage handling system uses a short UII because this needs to be read very quickly, but attribute data only needs to be read on baggage in the wrong locations. There is less of a challenge with long attribute data, because this is less likely to be read "on the fly".

There are two Registration Authorities that are key to extending the capabilities of RFID to support different applications:

- The Registration Authority for ISO/IEC 15961-2 is key to ensuring that object identifiers and other "data constructs" are registered. This allows RFID tags to be used in a reasonably generic manner, independently of the data content. In addition, the Registration Authority registers mapping tables that are used to achieve greater encoding efficiency on the RFID tag. These mapping tables have been designed to be machine readable, so that they can be embedded in interrogators to increase the level of automation and to rapidly support new applications as they are developed.

- The Registration Authority for ISO/IEC 15459 is also important, because one of the key features with many RFID tags is being able to – even requiring – the encoding of a unique item identifier. This particular register has enough capacity to be able to identify virtually any kind of object from any reasonable sized domain.

At present, even the existence of these Registration Authorities is known to very few organisations. Some responsibility rests with the vendor community to promulgate information about the benefits and issues. The registers[2] can provide an important source of information for achieving higher levels of interoperability.

7.10 Application standards

7.10.1 Overview

The application standards of any data carrier technology are independent of the technology standards, but should use them as normative references. They are usually developed by a user body with expert knowledge of the sector being addressed by the application standard. The quality of the technical knowledge varies from industry to industry; this is also true for bar code, but probably more so for RFID.

Another class of application standards, usually published as ISO standards, functions at a generic level and addresses a layer between the technology standards and the industry-specific applications. Effectively, these are "pro forma" standards that are designed to achieve interoperability between different domains using the same business functions such as a supply chain or transport interface. They do this by specifying or recommending a set of requirements. For RFID this often results in the specification of a single air interface protocol.

7.10.2 Key relationships with other components

The basic requirement for an application standard using an AIDC technology is to identify the data that needs to be encoded and the data carrier to be used. So, a fundamental first stage is to identify an appropriate data dictionary with the relevant data elements that need to be encoded. Additional characteristics that need to be taken into account are: whether the data element is mandatory or optional, to define any formatting constraints on input data, and whether the data is required to be permanently encoded or changeable on the RFID tag.

The RFID tag on its own does not comprise an RFID system, and consideration needs to be given to the air interface protocol being suitable in terms of expected performance to meet business requirements. Therefore, an application standard is required to select a particular air interface protocol, and furthermore to specify optional features in that protocol that are necessary to meet the requirements of the application. An obvious requirement is that the tag has sufficient memory to meet the encoding requirements, but the application standard might need to further specify either types of reading device or specific performance capabilities for the RFID system to work in a particular business situation.

Before standardisation, applications had to accept what was provided with respect to encoding schemes. Now, the choice of different schemes allows an application to make choices on the dynamics of the data within the application. If a fixed set of data is required, then some encoding schemes are better at addressing this and others can encode optional data in an extremely flexible manner.

Given the current state of developments of RFID application standards, the following additional components are sometimes overlooked, or given too little technical consideration. These include:

- The specification of minimum conformance requirements.
- The specification of performance, both as a minimum overall requirement and to meet expectations - in particular data capture environments.

[2] Register for ISO/IEC 15459: http://iso15459.nen.nl
Registerd for 15961-2: http://iso15961.nen.nl

- Device interface standards, although for some air interface protocols these still have to be addressed by proprietary technology solutions.
- Other infrastructure standards such as the data management and the higher level processes and applications.

7.10.3 Standards

A set of generic standards has been published by ISO in the series ISO 17363 to ISO 17367. These standards address, at a generic level, requirements for supply chain applications from the item level up to the sea-borne freight container.

A number of industry or sector RFID standards have been developed and published. Major standards cover the following sectors:

- The automotive sector for tyres (AIAG B-11) and returnable transport items.
- Baggage handling for air transportation (IATA RP1740C).
- Engineering parts for airlines and defence (ATA Spec 2000).
- Libraries (ISO 28560).

It is difficult to get details of these standards without having some inside knowledge to access information. The organisations, websites provide little information. In addition, we are convinced that other activities are taking place to develop RFID standards, but only minimum information is available in the public domain.

The GRIFS RFID Standards Database (http://grifs-project.eu/db/) provides details of the standards. Readers might be surprised that we have not included the EPCglobal application in this clause. It is certainly a major application but because the only data that is specified is in the Tag Data Standard, and there are separate air interface protocol standards, an **application standard** as such does not exist for the EPCglobal application.

7.10.4 Significant development areas

A number of industry sectors have pioneered the development of application standards and moved forward with implementations. IATA certainly has a commitment to apply RFID across a number of applications, starting with its baggage handling standard that was published in December 2005, work is nearing completion with engineering parts and in-flight catering.

The automotive industry kick-started its application standards with the AIAG B-11 standard for tyres, to meet certain legal requirements in the United States. The industry, through its regional trade bodies in North America, Europe and Japan, continues to work on the additional application standards. The AIAG B-11 standard has a revised scope and is now the *item-level RFID standard*.

The library community is interesting because it is migrating from proprietary applications to an open systems approach, and building on an extensive installed base. ISO 28560 (as a three-part standard) is in its final draft ballot, one step before publication. With 2500 libraries around the world already fully implementing RFID for all their stock items using proprietary or national standards, that sector is probably the first to address migrating from a set of proprietary RFID applications to a comprehensive standard. In parallel all the "pre-RFID" libraries face the challenge of deciding to migrate to RFID.

EPCglobal probably faces some interesting challenges as it addresses the encoding of attribute data on the RFID tag. In addition, the introduction of an EPCglobal tag at high frequency means that some significant choices will need to be made about hardware infrastructures. This issue is, effectively, similar to the challenges in the early days of the GS1 system when additional bar code symbologies were introduced. Then, the migration was from item level to supply chain applications; for RFID, the majority of migration is going to be from supply chain to item level.

An overall assessment of the potential for RFID application standards can be made by taking into account the numerous bar code application standards that have been in place since the 1970s. Not all are obvious candidates for RFID, but many are.

There are two major challenges that need to be addressed. There is a hierarchy of RFID vendors that creates a degree of remoteness and disconnect between the technology and business applications. The companies that make the integrated circuit (the chip) that is at the core of an RFID air interface protocol are often two or three steps removed from any interaction with applications. A classic example was the restriction of memory encoding capacity of the 18000-6C tag when it was first introduced. Tags with only the capability of a 96-bit unique item identifier were produced, which were focused exclusively on the then requirements of the EPCglobal system. Whereas IATA was able to make use of tags with this restricted memory in the initial implementations, the automotive industry had been completely frustrated for many years because it required more memory to encode its longer unique item identifier and to encode attribute data. Both the EPCglobal and ISO standards allowed for this, but the manufacturers failed to address the requirements of the industrial sector until recently. Still the choice of tag to meet these requirements is limited.

The problem does not only rest with the vendor community. Bar code is an obvious WYSIWYG technology that enables detailed practical demonstrations to take place, partly because each symbology has its own encoding rules. This means that an application can be delivered with a prototype solution at fairly low costs, especially given the wide range of data capture devices on the market. RFID presents a number of challenges that are fundamentally different:

- The encoding is invisible and, until the market expands, the ability to demonstrate this is at best like a 'black box' and often a question of trust.
- The choice of data capture device, and even the tag design can impact performance.
- Interoperability is not proven for the more demanding industrial applications with mixture of tags, readers and data content volume.

7.11 Environmental regulations (e.g. WEEE, packaging waste)

7.11.1`Overview

The Directives that are discussed in this clause have some small direct impact on RFID, as will be discussed below. Their greater impact is on potential applications using RFID to implement the Directive or to assist in the management of systems associated with the Directive.

7.11.2 Key relationships with other components of an RFID system

There are three standards (the details are discussed below) that have a direct relationship on the use of RFID technology.

- Waste electrical and electronic equipment (WEEE).
- Restrictions of the use of certain hazardous substances (RoHS).
- Packaging and packaging waste.

It is generally accepted that interrogators and active RFID tags fall into the category of "electronic devices" as defined by the WEEE Directive. On the other hand, passive tags are accepted as being outside the scope. As battery-assisted passive tags are introduced, consideration will need to be given as to how they are categorised. They may depend on the nature of the battery technology. This will present an interesting challenge for interpretation. The Directive states that "If RFIDs are put on the packaging of the electrical and electronic equipment, they are considered to fall outside the scope of the Directive because they are part of the product that is not covered by the WEEE Directive." However, batteries themselves are probably within the scope.

The RoHS Directive restricts the use of certain toxic materials that were once reasonably common in electrical and electronic equipment, specifically: lead, mercury, cadmium, hexavalent, chromium, polybrominated biphenyls (PBB) or polybrominated diphenyl ethers (PBDE). As the 2002 Directive required that from July 2006 these materials shall not be used in electrical and electronic equipment, the Directive should have been implemented by all product manufacturers. RFID products in Europe shall not contain these materials.

The Packaging Waste Directive means that whereas RFID tags applied in packaging are exempt from the WEEE Directive, depending on their proportionate relationship with the packaging, this Directive may have some minor impact on the use of RFID.

7.11.3 Significant development areas

Although the RoHS Directive has a very narrow definition, the handling of hazardous material within the supply chain has significant environmental and health and safety issues. There are already facilities within the ISO RFID data standards to be able to identify hazardous materials in a general supply chain environment, so that they can be selected and processed separately and in a safe environment.

If RFID tags are applied to electrical and electronic components, then they have the prospect of contributing to systems that can deal with the recovery and recycling of those items.

As more and more products carry RFID tags at the item level, such tags are likely to be applied – even incorporated – into the product packaging. While some types of packaging can be easily distinguished from others (e.g. cardboard from glass from plastic), sorting different types of plastic can be slightly more challenging. There is the long term prospect of RFID tags that are applied to high volume plastic packaging to enable such products to be sorted using the basic look-up to sort that type of packaging. A proposal has been submitted by CEN/TC 225 to the Commission to create a CEN Technical Report for sorting spare automotive parts at the end of their life.

There are a number of other Directives that lend themselves to RFID applications in general and specialised supply chains. The ones in the general supply chain are food and pharmaceutical traceability, and in the specialised sectors critical safety components for aircraft and the automotive sector.

7.11.4 Regulations

The GRIFS RFID Standards Database (http://grifs-project.eu/db/) provides more detail of three Directives:

- 2002/96/EC WEEE
- 2002/95/EC RoHS
- 94/62/EC Packaging and Packaging Waste

7.12 Data exchange standards and protocols

7.12.1 Overview

Our definition of data exchange systems is intended to cover indirect communications between partners, usually through some hub mechanism. We exclude any direct peer-to-peer communication and any data exchange that can be implemented with in-house systems.

7.12.1.1 DNS as a reference

A reasonable analogy to use as a reference is the access to websites through the Domain Name Service (DNS). The DNS uses one of the original Uniform Resource Identifiers (URI) for the Internet, namely the Hypertext Transfer Protocol (HTTP). If we take an example of a website address, then the basic DNS model can be explained.

http://www.cen.eu

The basic idea of a URI such as this is to provide a name that is understandable by humans but, for communication over the internet, this needs to be communicated in the form of an Internet Protocol (IP) address, using an IPv4 or IPv6 address format. The character string 'http' identifies the URI system, where the DNS with the appropriate algorithms for resolving the namespace for 'http'. For reference, the common term "URL" should specify a specific location on the Internet but as this is increasingly not the case, the term URL is deprecated within the Internet Engineering Task Force.

The character string 'eu' is behind a dot (full stop or period), and identifies what is known as a country code Top Level Domain (ccTLD). True Top Level Domain examples are 'com', 'org', 'net', and 'info'. A TLD or ccTLD has a sponsoring organisation and registry, in the case of .eu, this is an organisation called EURid.

EURid has a number of name servers that are used to resolve (convert) a URL into an IP address. The string 'cen' is in the next level of the search, and any enquiry is routed from the DNS resolver for the domain eu to an IP address(es) that hosts the CEN website. Once on the CEN website, individual pages can be called up either from the menu or directly from the enquirer's web browser by using the forward solidus (/) as part of the syntax to resolve and return the specific page being requested.

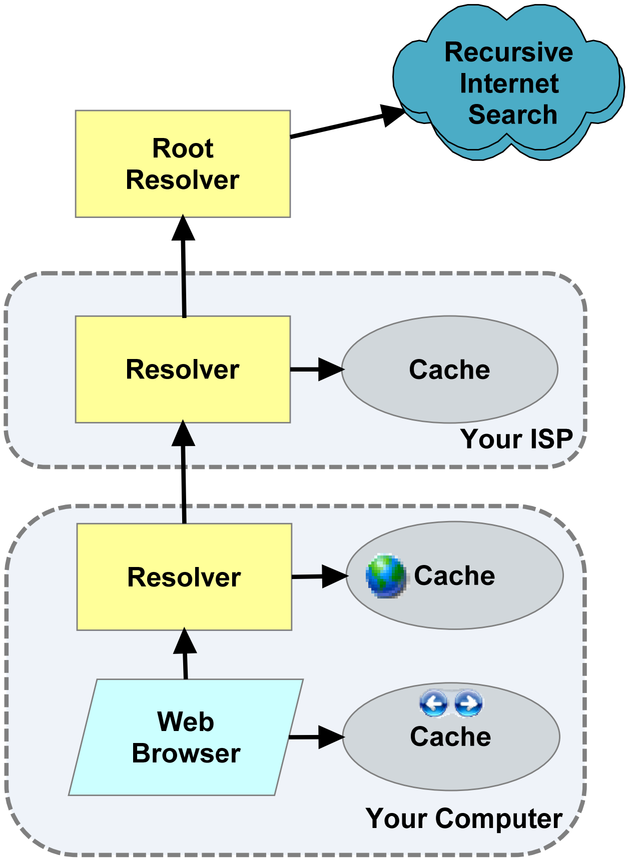


Figure 11: A typical web search

The figure shows that the number of pages that can be cached is relatively small at the browser level, and increases at the computer level. We have used the 'back' and 'forward' symbol to indicate browser and 'history' icon to indicate computer, neither of which is technically accurate, but points to the difference in scale. If the ISP cannot resolve the web address, then it sends a request to the TLD to start a recursive search process – all of which takes a fraction of a second.

The reason for giving this elaborate explanation around web pages is to indicate that so long as a hierarchical structure exists, it is theoretically possible to resolve any form of address. Other higher level URIs include **mailto** used for transmitting e-mail addresses, **ftp** for file transfer, and **urn** the Uniform Resource Name, which is discussed in greater detail below.

7.12.1.2 Uniform Resource Names

As mentioned above, the Uniform Resource Name (URN), is a sub-set of the Internet URI scheme. A number of sub-divisions of URNs have been registered for use on the Internet under what is known as a URN namespace with a namespace ID (NID). Some that are relevant to this report include (in order of original registration): oid, isbn, swift, nfc, epc, epcglobal. These are a few of the 40 formally registered URN scheme. There is even a proposal for a URN for ISO, which is not yet on the register.

The basic requirement is for some namespace code to have a hierarchical structure so that the code can be passed through a recursive resolution system. The resolver algorithm takes the highest level component of the code (which as shown with the DNS system described above) does not have to be numeric and resolves this to a root resolver. Then, the resolution process continues to the next tier in the hierarchy, with each tier separated by some syntax character.

Just as with a web browser, functions for processing a urn through a urn resolving application may be shared between:

- the resolver (generally – but not always - with public access, as will be discussed below) to gain access to the IP address
- a host system that provides the detailed information (that might be partly or completely restricted except to those with permission for access).

7.12.1.3 Additional context for RFID and the supply chain

Web sites and information held with other URI schemes are not always required to be updated dynamically and in real time. New web pages are added on an occasional basis, and e-mail addresses – even for large corporations – change fairly slowly.

In contrast, there are some significant expectations of making RFID data available on the internet. Some information may be fairly persistent in its association with a product (e.g. name, country of manufacturer, ingredients). Other features are likely to be associated with the serialisation of a product or other objects in terms of its unique item identifier, so the time, location, custody of an item as it moves through the supply chain changes with the passage of time.

In turn, this means that information about any individual object is unlikely to be centralised, but distributed in various data repositories associated with the chain of custody. A retailer will probably know which individual customer purchased a domestic appliance, and either the customer or the retailer might share this with the manufacturer for warranty purposes. The customer would certainly have no access rights to know of other customers who purchased the product, nor the difference between the ex-factory and retail point-of-sale price. The net effect of this is that some new principles will need to be part of every data exchange system for objects:

- A partitioning of a code structure for resolution, so that an IP address is identified (typically) to the product level but not to the unique instance of a product. This type of structure is already available as the difference between a web site URL and the address of a particular web page.
- The need for authentication and permission to access particular type data, something that is already available on the web and invoked at the web site level.

- An increased level of distribution of data associated with a particular unique item identifier. This requirement (discussed in more detail below) means that individual organisations will have the dual role of making enquiries for more information associated with an object, but will also be the source of information from external enquiries. Although this type of information is available between pairs or small groups of trading partners, the prospect to develop something like the Internet of Things requires a greater level of data exchange at a significantly lower level of granularity.

7.12.2 Key relationships with other components

Figure 12 shows the relationship of data exchange from the point of processing object data and sensor data.

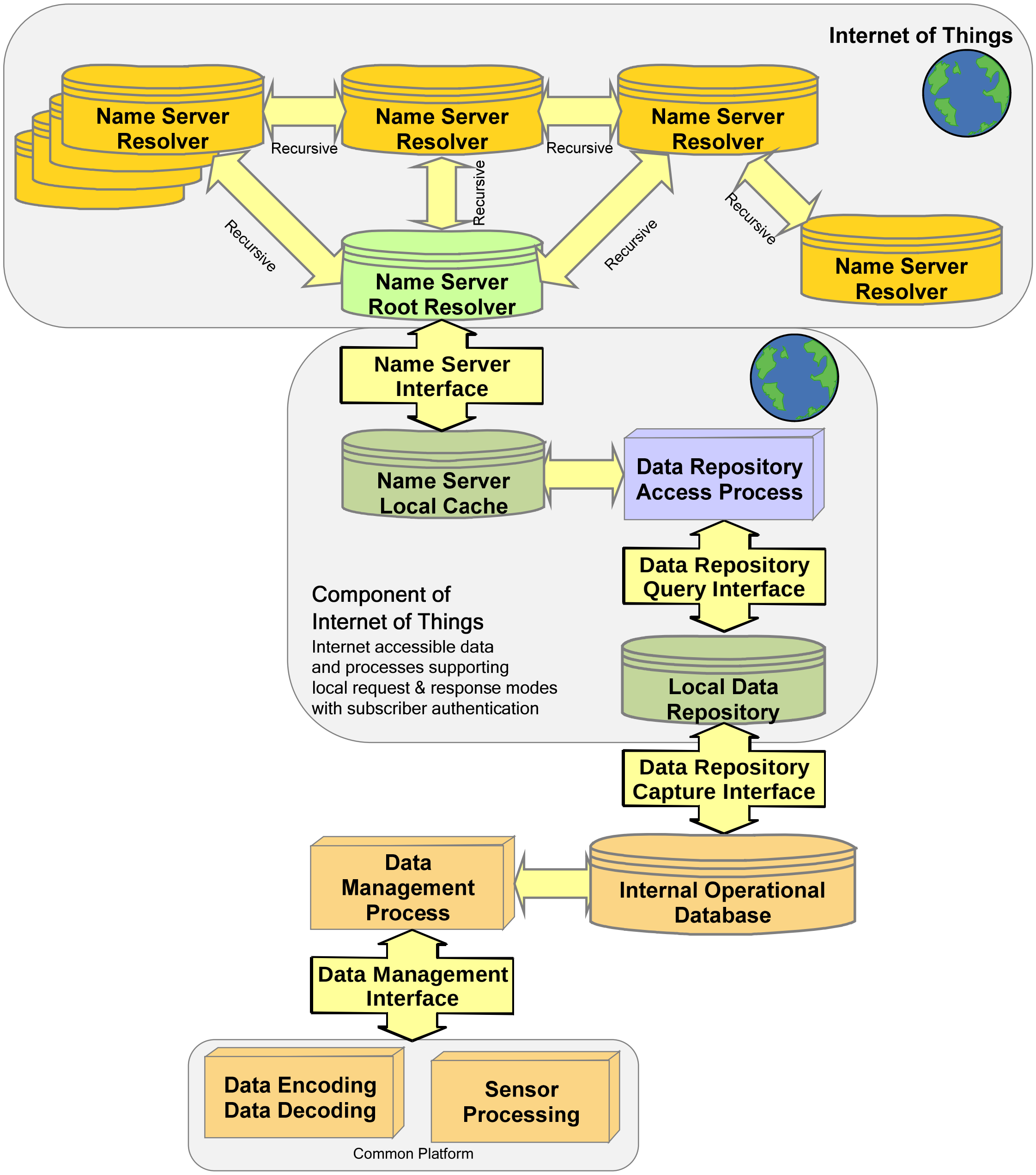

Internet of Things
Name Server Resolver
Name Server Resolver
Name Server Resolver
Name Server Resolver
Recursive
Recursive
Recursive
Recursive
Recursive
Recursive
Name Server Root Resolver
Name Server Interface
Name Server Local Cache
Data Repository Access Process
Data Repository Query Interface
Component of Internet of Things
Internet accessible data and processes supporting local request & response modes with subscriber authentication
Local Data Repository
Data Repository Capture Interface
Data Management Process
Internal Operational Database
Data Management Interface
Data Encoding Data Decoding
Sensor Processing
Common Platform

Figure 12: Data exchange: interrelationships

The data management processes create whatever internal operational databases are required to make the organisation function properly. Details of this are beyond the scope of this report. However, such resources are the prime source of what is held within the organisation on the local data repository to share with others who have access on the particular name server. This name server could be part of an EPC system, or an IATA information system for baggage handling, or an automotive system for tracing components for manufacture to after sales repairs, or any other data exchange system.

This local data repository requires an interface standard to determine what generic business data needs to be placed in the local repository. The repository may then require additional data, by initiating queries through an access process system, locally accessible name search, or through some interface to an external route named server.

The process can also be applied in reverse, where an external source can request data that is on the local data repository. This part of the system is significantly more elaborate and complex than that of a web master adding new pages onto a web site.

All the external communications are through a name server root resolver that has the IP addresses of other name server resolvers that can provide the next level IP addresses. The process is recursive, moving from one resolver to another until an IP address is found that can provide all the information being sought by the original query.

7.12.3 Standards

EPCglobal is reasonably advanced with its development of standards for data exchange:

- The EPC Information System Standard fulfils the functions defined in Figure 12 as the Data Repository Capture Interface and Query Interface.
- The Object Name Service Standard is an interface standard that is equivalent to the Name Server Interface.

Another data exchange system pre-dates EPC. This is the **Handle** system that provides a global name service particularly for media products. This is part of a larger system known as digital Object Identifiers (DOI), which provides a digital identifier for any object of Intellectual Property. Recently, the DOI system began to be standardised as ISO 26324 *Information and documentation – Digital object identifier system.*

Both the EPCglobal ONS system and the DOI system make use of various standards and protocol defined by the Internet Engineering Task Force (IETF). Documents are published in the form of a Request for Comments and, even when approved, they retain this naming convention. Two particular RFCs are relevant for accessing data over the Internet:

- RFC 3986 Uniform Resource Identifier (URI): Generic Syntax.
- RFC 3403 Dynamic Delegation Discovery System (DDDS) – Part 3: The Domain Name System (DNS) database.

For the internet to be used to resolve a Unique Item Identifier, the hierarchical structure needs to be converted into a domain-name, usually by stripping off any serialised component. The conversion algorithm from UII to domain name is part of the specification of the particular URI scheme. Once the local resolver has created this domain name format, a DNS query is issued for NAPTR records for that domain. The processes defined in RFC 3403 return URLs that point to services that can provide the information.

The GRIFS RFID Standards Database (http://grifs-project.eu/db/) provides further details of these standards.

7.12.4 Significant development areas

The EPCglobal Object Name Service (ONS) is a significant development for using the Internet as part of the data exchange system. Standards and tools are already in place to support this function.

Many observers have assumed that ONS is the only form that can be used to make use of the DNS resolution system. This is not true, and any formally registered URI – including specific URNs (like the EPC codes) can be used. The granularity both of the resolution system and of the associated data is defined within the IETF RFC for the particular URN. Whereas, for retail purposes, a book might need to be identified to an instance of a particular product, the **urn:isbn** only identifies to the title or specific edition of a title.

The Digital Object Identifier (DOI) has been mentioned in this clause, but readers need to be aware that it only deals with objects associated with Intellectual Property. However, we understand that there are over 4 million such objects as part of the system, and also understand that the Commission of the European Union uses the DOI system for identifying many documents. As such a significant system (probably with more records and more users than ONS) it provides an alternative model that might have components that are relevant for other domains.

Given that most Unique Item Identifiers that are compliant with ISO encoding rules are based on object identifiers, a solution needs to be developed for this major class. Some form of generic model is required. This then needs to be supplemented by, as follows:

- Domain-specific syntax and mapping rules from the UII to the DNS format.
- Based on this syntax, specific capture and query interface standards need to be developed to access information on the local data repository.
- The Name Server Interface (equivalent to the EPCglobal ONS standard) also needs to be developed.

Our research has identified that the URI scheme can offer high degrees of flexibility and the amount of disclosure that is required to satisfy the IETF can vary, depending on the domain. For example, **urn:swift** provides very little information about the structure of its URI, except for the higher level of the hierarchy. This ensures that while this URN can be identified by a "non-SWIFT" resolver in the sense of delivering appropriate error codes, only compliant SWIFT resolvers are able to deal with secure banking data. Further research is required to establish whether some aspects of a resolution service need security, in addition to subscriber authentication and permission rules.

7.13 Security standards for data and networks

7.13.1 Overview

There are four zones in an RFID system where security features can be considered and applied:

- **The RFID tag itself**: Some levels of security can be built into the tag, with obvious features being the locking of data so that it is permanently encoded, and the inclusion of password matching before permitting subsequent transactions.
- **The air interface protocol**, which can support features in the command structure to the tag, such as passwords and security keys that can restrict unauthorised access, particularly to write data to the tag. There is also the additional security aspect of unauthorised reading, but most current RFID applications (like those of bar code) tend to provide an open access to the reading of data. Encryption techniques can be used to make it impossible or extremely difficult to interpret data that is read, and this applies to bar code and RFID. Developments are possible to restrict the reading of some sectors of memory.
- **The RFID interrogator** (reader) which, with unauthorised emulation, might provide access to the network containing more sensitive data.
- **The network itself**, which some experts consider is fundamentally equivalent to any form of network security, while others argue that RFID data presents a special case. Our view is that it is really the new types of application that present network security problems, especially if security features are implemented at lower levels of the system.

7.13.2 Key relationships with other components

Security has been somewhat of a "Cinderella" feature of RFID systems, generally ignored or reduced to a minor role until recently when its relevance appears to be manifesting itself. We consider the limited number of standards in this area (below) but, for now, we want to focus on some of the basic practicalities.

Apart from features such as locking part of the memory on an RFID tag and low-level password control, there are very few security features built in at the tag level. Also, while most tags do support selective locking, the notable exception was the first generation of the ISO/IEC 18000-6C tag, but this was the only tag that provides support for passwords. The current EPCglobal C1G2, and current Final Committee Draft of ISO/IEC 18000-6, support selective locking in one of the memory banks. It will be some time before the first generation tags are no longer manufactured and even longer before they are no longer used in applications.

Even with smart cards, the security aspects are often provided as part of a product implementation and can even be proprietary. So, in the recent hacker attack on smart cards, it was not the SC17 standard that came under criticism, but a proprietary product.

Some aspects are independent of tag technology, and the data protocol standards provide advice about encrypting data but retaining object identifier references. Such an approach places very little burden on the RFID system, other than requiring possibly more memory and air transmission time, with all the processing burden carried by the interrogator and higher level systems. We know of no implementations of this feature. We are aware that other mechanisms are being considered for standardisation.

To improve the situation with respect to tag hardware security, a New Work Group has been established by SC31 in June 2009. Work is currently under way to develop ISO/IEC 29167 to add security features to RFID tags. Although the title of the standard implies adding security services to any ISO/IEC 18000 series tag, the only tag included by normative reference is 18000-6 and particularly Type C. These security features could probably be implemented in 18000-3 Mode 3 tags, but it is not clear what can be achieved with other tag technologies. As the Work Group is only a few months old it is difficult to assess its scope in the long term, but it has achieved significant progress in a short time.

In the RFID air interface, there is little security other than the link within the reader zone, passwords - where implemented, and ongoing "handshake" of being able to talk to a specific tag. The handshake feature is really to ensure proper communication during authorised communication and while it can be considered a security feature, it does little to protect against unauthorised communication. In fact, most air interface commands are of a very low level bit-based structure that are easy to construct. Even with systems that use passwords, once a communication channel has been established, the assumption is that all subsequent commands exchanged with the particular tag are secure and the password is often not invoked in subsequent commands that are part of the communication chain.

RFID interrogators are often considered to be just another network device and are provided with Internet Protocol (IP) addresses to enable communication. If authentication is not part of the communication process, then it is relatively easy to achieve unauthorised interrogator emulation.

From our limited access to application standards, there is little information in these about security.

7.13.3 Standards

We have identified two ISO standards from JTC1/SC31 that are relevant. Details of these are provided in the GRIFS RFID Standards Database (http://grifs-project.eu/db/) and we provide a basic overview here.

- ISO/IEC TR24729-4 is a Technical Report that is being developed to provide guidelines on Tag Data Security
- ISO/IEC 29167 is a new work item addressing air interface for file management and security services for RFID

There are obviously many network security standards in place and, without detailed expert knowledge of the particular standards, it is difficult to cite specific ones as being relevant to RFID network systems. However, we would point to the general standardisation area of ETSI as being a prime source for more detailed work to identify relevant security standards.

7.13.4 Significant development areas

The new SC31 WG7 Security has been working previously as a Sub-group of SC31 WG4, and so was able to begin its work with a flying start. The first standard, ISO/IEC 29167 could be a comprehensive document, and the key test will be the extent that features are added to the RFID tags, interrogators, and higher layers including software. Already there are implications for the data protocol, particularly if different "sectors" of memory support different security features and access to read and write data.

In clause 7.3 we indicated that there can be significant misunderstandings about the ability to add new features to an RFID tag technology that is already standardised and has compliant products in the market place. Security features have a direct link to privacy features, even though they might not necessarily be the same. Adding security features to established RFID technology can only be done on an optional basis unless all previous versions of compliant products are considered to be non-compliant. The only way security can be incorporated as a mandatory feature is with the development of a new air interface protocol.

This means that the work to develop standards for security that are only applied retrospectively is, at best, sound advice. One way to overcome this is for application standards to provide additional mandated compliance requirements that result in the selection of RFID products that have security features that are otherwise optional in the technology standard. The advantage of this application mandate approach is that the marketplace can have an influence on the availability of products. There are two constraints on this:

- Those developing application standards need to have a significantly better understanding of RFID security issues.
- Until the first technology vendor incorporates security features, an application has a fundamental choice of not adopting RFID or compromising its high standards and downgrading the security aspects. We cite an example of the lack of power of the end user marketplace, or the lack of understanding by vendors. Many manufacturers of ISO/IEC 18000-6C tags failed to address the requirements of the industrial community by not providing encoding capacity in Memory Bank 11, and a larger encoded capacity in Memory Bank 01 (other than that required for basic EPC applications). The fact is that the vendors missed out on two or more years of potential marketplace development in sectors like automotive, baggage handling and other primary sectors. It is only in 2008 that users in these sectors have been able to procure RFID tag products that meet their requirements.

CEN TC225 did propose to the European Commission in May 2007, a project for an RFID standard that addresses security aspects. This was to have a particular focus on identifying weaknesses and gaps in the present standards and technology, and with a view of providing security features elsewhere in the RFID system to help compensate for these. Whilst discussions on this proposal (and others addressing application areas) continued until summer 2008, the Commission decided instead to issue a standardization Mandate[3].

This constitutes a more significant initiative – it requests the European Standards Organisations (CEN, CENELEC and ETSI) to prepare an overall framework for future standardization in the field of information and communication technologies applied to RFID systems. We abstract below a paragraph from the Mandate, which aligns with what we have included in this clause:

[3] A “Mandate” is a request (rather than an instruction) to the European Standards Organizations for specific work – it is up to the ESOs whether or not to accept.

> "Many organisations have a tendency to look at RFID security in the rear view mirror, i.e. rushing to find a solution to a security problem after it has happened. Such behaviour can no longer be contemplated as emerging security threats, combined with the increased use of and dependence on RFID, leave organisations in both the private and the public sectors with an obligation to plan, design and implement clear strategies."

The Mandate is to be implemented in two phases, again abstracting from the Mandate itself:

> **"Phase 1.**
> The objective of the first phase is to prepare a complete framework for the development of future RFID standards. This framework will include a detailed standardisation work programme in response to the identified gaps. The standards will refer to all elements of the RFID value chain, from the tags themselves – power levels, reading distances, encryption tradeoffs, to the architectures and services relevant for the networking of tags – security frameworks, object naming, tracking, and addressing, etc. Appropriate use of intermediate results from relevant EU funded projects (including GRIFS, CASAGRAS) shall be made.
>
> Particular attention would need to be given to the likely technological evolutions to be expected in this domain especially in the perspective of the future Internet of Things, and the requirements (including openness and interoperability) to cope with environments where networked tags offer significant functional capabilities beyond what is state-of-art today.
>
> The resulting standardisation work programme will be submitted to the Commission services, which will consult the Committee 98/34.
>
> **Phase 2.**
> The objective for the second phase is to implement the standardisation work programme agreed upon in the first phase. The execution of the specific standardisation tasks shall be carried out in close co-operation with all relevant stakeholders."

Within three months of the Mandate being agreed, the European Standards Organisations are expected to identify their arrangements for co-operation to address the Mandate. Then, after a further nine months, Phase 1 is intended to be completed, which could well result in specific standards work in the three standards-making bodies.

At the time of writing, the Mandate has been approved by the EU Member States and formally accepted by CEN, CENELEC. The ESOs are in the process of appointing the experts to execute the Phase 1 work. This activity will clearly use the present GRIFS Report as one starting point.

7.14 Real time location standards

7.14.1 Overview

A Real Time Location System (as defined in ISO/IEC 19762-5) is of a combination of wireless hardware and real time software that is used to continuously determine and provide the real time position of assets and resources equipped with services designed to operate with the system.

A number of fixed location nodes are used to determine the relative location of the RTLS tags attached to the assets whose location is being determined. One of various techniques is used to achieve this, including: time travel, differential time travel, and time travel triangulation.

7.14.2 Key relationships with other components

There is some possible overlap and ambiguity with RFID active tags. The main differences are:

- In an RTLS system, all the items that are being tracked are generally known to the application and are expected to remain within the physical bounds of the RTLS system. This is often a building such as a hospital, office, factory, warehouse, or storage yard with all the capture points connected on a local network. As such the position of RTLS tags is monitored continuously.
- In an active RFID system, the tags are only read when they come within appropriate communication range, and transmit their identity and other data when within the reading zone. Between reading zones the only "active" function is to maintain any sensor process, if included.

The differences are fairly subtle, and there are likely to be RTLS systems that make use of RFID tags in the following way. If once an RFID tag is within a clearly physically bounded site and its presence is exposed to the entire space domain of that site, then RFID tags and the system might be able to provide some degree of location using basic RTLS techniques.

Equally, RTLS systems might be capable of providing some of the same functionality of active RFID tags. If a limited number of sites are involved in an application, then each site can be set up with an RTLS system. As long as the data that is transferred between sites includes a constant identifier, then each site is capable of tracking the location of the item when within its zone. The extent to which RTLS might encroach on RFID is determined by the fact that there are proposals to extend some of the ISO standards to support the sensors.

7.14.3 Standards

The main ISO standards that have been developed for RTLS have been the work of JTC1 SC31 WG5. The standards cover: application program interface, various short-range (as opposed to radar and satellite-based systems) and conformance and performance methods for systems operating at 2.4 GHz.

7.14.4 Significant development areas

A review of news in the technology press and company product information indicates a trend to overlap applications in the marketplace between active RFID and RTLS. However, from a standardisation point of view, there appears to be no convergence given the fundamentally different air interface protocols and preferred frequencies. Most active tag technologies operate at 433 MHz, while most RTLS systems operate at 2.4 GHz.

Some RFID vendors are adopting or adapting RTLS concepts to provide additional functionality for their products. This is even extending to claimed developments in passive backscatter RFID tags. Such developments will probably remain proprietary or, if not covered by IP, will still result in product differentiation. Again, this is unlikely to have a direct impact on the standardisation effort other than being an indicator that some RFID features that bring benefits to end users are beyond the scope of the standardisation process. However, the biggest concern is the potential confusion about RTLS and RFID among those developing application standards.

7.15 Mobile RFID

7.15.1 Overview

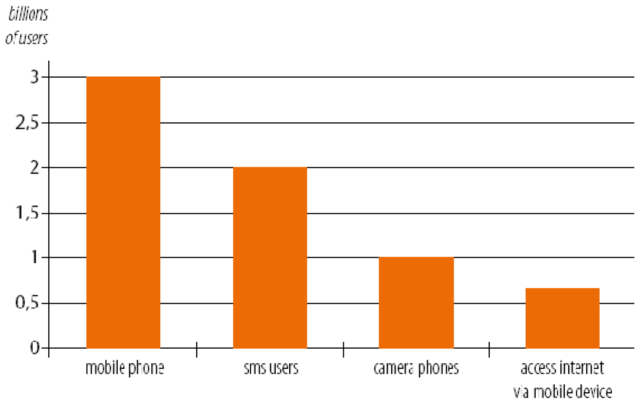
The potential to read RFID tags with mobile devices has always been possible in the industrial and commercial sector. In contrast, the use of RFID tags and mobile phones presents a possible exponential growth in the number of RFID data capture devices that will be available. Technology vendors within the Near Field Communication Forum, with a separate and different initiative from Korea, will be the main drivers to achieve this.

This represents a paradigm shift in potential applications for RFID, both in terms of adding functions to proposed RFID business applications such as item level coding, and creating new applications such as using RFID tags to provide a look-up reference to location information.

The work is fairly diversified and, in this clause, we concentrate on some of the generic issues and the specific work of JTC1 SC31 WG6.

7.15.2 Key relationships with other components

At a fairly basic level, adding RFID for data capture on a mobile phone is no different to one of the traditional portable hand-held reader companies introducing a new product. However there is a significant difference in the potential scale of market penetration, as shown from the following data.



Source: TNS Mobile Trends Guide 2006,
Computer Industry Almanac
Tomi Ahonen Jan 2007

Figure 13: Mobile phone functions

There are some technical and social issues that need to be considered:

- Because mobile phones are devices that can be purchased by the general public, the potential for new applications is significant. These will either extend the benefits and functions of RFID tags that will already be in place, such as being able to read a tag on a food item and using some look-up service to identify whether any of the ingredients present potential allergy problems to a consumer. New applications will include using RFID tags as reference points for geo-location within towns and cities either for tourists or for people with disabilities.

- Given that there are very few air interface protocols, and with current targets on mobile phones being focused on 13.56 MHz (NFC) and UHF (Korean perspective), mobile phones will be able to read any RFID tag compliant with the air interface protocol installed in a mobile phone. Generally speaking, reading an RFID tag is not considered to be a problem for security or confidentiality in open system supply chain activities.

- A more significant concern is the potential capability of mobile phones – in the hands of anyone – being able to re-write data on an RFID tag. Given the low levels of security with RFID, this could pose a problem for tags that are generally exposed to the public.

- A similar challenge exists with the fact that the mobile phone – particularly the NFC concept of using the phone as an electronic purse – acts a tag emulator. Used for legitimate purposes in well-defined applications, this will increase potential benefits. Again, the problem is with the fact that the mobile phone tag emulator in an application not designed to support this will, at best, treat such a "tag" as one from a different domain/name space. A more concerning scenario is if the application has no means of filtering out tags from other domains or, worse still, if the mobile phone is used as a means of either hacking into or attacking the application.

We also note a potential divergence in the starting positions of the two main groups developing standards. The Near Field Communication Forum built its original structures based on ISO/IEC 14443 operating at 13.56 MHz. It also supports the Japanese FeliCa (JIS X6319-4) also operating at 13.56 MHz. In contrast, the initial focus from the Korean proposal to SC31 has been on UHF technology operating at 860 to 960 MHz.

7.15.3 Standards

A number of ISO standards have been approved as work items since the first edition on this report, none have yet been approved for publication, but this might be achieved in 2010. Details are in the GRIFS RFID Standards Database (http://grifs-project.eu/db/).

The Near Field Communication Forum has also published a number of standards. We include details of one in the GRIFS RFID Standards Database (http://grifs-project.eu/db/). Details of others are available from the following URL.

http://www.nfc-forum.org/specs/

7.15.4 Significant development areas

Our initial research on the NFC Forum standards indicates that there is no support for **urn:oid**, and the support for the EPCglobal standard appears to be based on the direct encoding of the **urn:epc** (and variants) and not the basic EPC code.

Our analysis of the New Work Item proposals for SC31 indicates that, as presently focused, the ISO standards might not be capable of reading EPC codes directly encoded in an RFID tag, nor unique item identifiers compliant with the ISO/IEC 15962 encoding rules.

If our limited analysis is correct, the major format for encoding unique item identifiers is not directly addressed by these two mobile phone initiatives. The parallel, sometimes diverging, activities of the Near Field Communication Forum and JTC1 SC31 WG6 require further investigation, which might be better undertaken within the CASAGRAS project, as some of the developments are beyond the scope of supply chain activities.

In addition, there is a further risk of divergence given the preferred focus on air interface technologies:

- With the NFC Forum supporting 13.56 MHz (ISO/IEC 14443).
- The SC31 WG6 standards being focused on UHF technology.

A final development area that needs to be taken into account is the recent GS1 Mobile Communications initiative, which is considering both RFID and bar code data capture.

8 The standards map – including assessment of relevance

As described in Clause 1.3, the starting point for this study has been the RFID architecture model. Following this model, a spreadsheet was created with standards in the following areas:

1. Frequency regulations
2. Health and Safety regulations
3. Data protection and privacy regulations
4. Air interface standards
5. Sensor standards
6. Conformance and performance standards
7. Device interface standards
8. Data encoding and protocol standards (often called middleware)
9. Data standards
10. Application standards
11. Data exchange standards and protocols (e.g. DNS, ONS, Handle)
12. Security standards for data and networks
13. Real time location standards
14. The European Harmonisation procedure
15. Mobile RFID

Although the focus of the study has been on standards, several aspects of the RFID architecture model involve regulations as well. Wherever possible, relevant regulations were included in the spreadsheet. By following the RFID architecture model the spreadsheet allows an understanding of the interrelationships between standards (and certain regulations) in various areas.

A prerequisite for drawing these interrelationships is the accuracy of the data in the spreadsheet. Whereas a significant amount of time has been spent to identify the available standards in a certain area of the RFID architecture model, it turned out to be very difficult to obtain all relevant information that should be available on a standard. Since the development of standards progresses in time, it became clear that some information in the spreadsheet should already be updated.

These two problems related to the accuracy of the data in the spreadsheet not only apply for creation of the spreadsheet but will certainly apply for future revisions of the information. This would argue for a decentralised maintenance of the spreadsheet once members of the Forum are identified. This will enable experts closer to each of the projects to provide more accurate and up-to-date information about a standard. For standards that are not yet published or being revised, the database contains a best estimate of the date of publication from information in the public domain.

Since the publication of the first edition report all the information on the spreadsheet (which was incorporated in annexes to that report) has been transferred to an online database that can be updated more dynamically. The GRIFS RFID Standards Database (http://grifs-project.eu/db/) provides up-to-date information on RFID standards. To make it easier to search the database, each standard is classified in three main categories:

- **The area of application**, i.e. to which hardware or software area it is related
- **The organisation** that published the standard
- Its **current status**, whether it has already been published or is still under development

This is a publicly available source of information allowing the database to be searched using the above criteria. Additionally, there are descriptions of each standard category and publishing organisation on separate pages.

9 Key future drivers, constraints, comparisons and gap analysis

9.1 Pervasive networked systems – the Internet of Things and RFID

We are using as our reference for the Internet of Things that which seems to be gaining acceptance within the EU Commission.

> "A world where physical objects (dumb or smart) are seamlessly integrated into the Internet, and where the physical objects can become active participants in business processes."
>
> Dr. João Schwarz da Silva
> Director
> "Converged Networks and Services"
> European Commission

We would add that this network is not limited to business processes. Eventually various types of "edge devices" will be capable of linking to the Internet, or an Internet-like service extending benefits and applications to business users, customers, and including services for individual citizens.

Because this report focuses on RFID in the supply chain activities, we will focus on this narrower scope.

9.1.1 Future drivers

The prime focus on resolver services will be on a business-to-business (B2B) basis. Once these services become established on a B2B basis, there is no doubt that some services will extend to individual consumers. Our assessment is that it will be some time before the business-to-consumer (B2C) services can be cost-justified in their own right. However, there is one paradigm that can invert the logic of rolling out services to consumers at some distant future date. If mobile phone technology develops to support reading of RFID (we discussed some of the issues in clause 7.15, and again in 9.7), then a readily available infrastructure will be available at fairly low cost to industry providers – whether these are manufacturers of the objects to which RFID tags are applied, retailers, or information providers.

One scenario that follows on from this is that the unique item identifier (in this case the EPCglobal code) could be resolved in a manner as intended through the ONS system. Another scenario is that the code could simply be captured and treated as a code that was used in an application that was resident on a mobile phone. Such applications could even apply to the capturing of product bar codes, using the camera and an embedded scanner. Similar infrastructures could be established on computers in the homes of individuals.

In the original edition we noted the recent launch of Tikitag by Alcatel-Lucent. This is now one year old and has been re-branded as Touchatag (http://www.touchatag.com). The core to the service is a network-based application correlation server using 13.56 MHz tags compliant with NFC applications. The starter kit, including a USB tag reader and 10 tags, costs 29.95 EUR + tax and additional tags can be purchased in batches of 25 at 19.95 EUR. A fundamental difference is that the identifier is the unique chip ID in an ISO/IEC 14443 tag, and the owner of the Touchatag maps this to a specific URL of their choice, which could even be of the format: http://www.myhouse.info. Any of the top level domain names could be used, including country code domain names. Many of the applications and submitted ideas seem to be associated with automating a basic function like opening a given web page or calling a particular Skype phone. With about 150 applications, this is still a novelty.

9.1.2 Constraints

There have also been arguments associated with the future of the Internet that, irrespective of whether the world replaces copper wire with fibre optics, there is still a requirement to go through computer gateways. If the apparent "free-for-use" network is insufficient to meet the requirement for commercial look-up purposes, then the trade-off will either be lower service, or the need to provide a robust service for separate, paid-for, networks.

The most difficult constraint will be a combination of competing new applications for the Internet, or ones that are rapidly adopted by popular demand among individuals. As an example, SPAM accounts for 90% of the traffic on the **mailto** Uniform Resource Identifier, whilst streaming downloads of various types of media is on a rapid increase. Now that these are established features of the WWW, it is possible to assess their future impact. Ten years ago, even five years ago, predictions of the use of these features would have been very unreliable. The only certainty is that new features will be developed and marketed, which increase the demands on the Internet.

9.1.3 Comparisons and gap analysis

Apart from the need to trace an individual item, there are countless applications that only need to identify the product for the purposes of a look-up service. Given that the structure of the EPC SGTIN code is itself based on the GS1 GTIN code represented in bar code, the possibility of creating an Internet of Things from bar code data capture has nominally been available since the development of the DNS system. Certainly, a core system similar to that of Touchatag, has long since been possible; for example by reading a bar code and looking it up on a service such as http://www.nutallergies.eu.

In summary, there appear to be a variety of ways to move forward, of which we have identified three options:

- Associating a tag identifier, or some other encoded identifier with a URL on a system similar to Touchatag, with a look-up facility. Further research is necessary on this particular system to identify any proprietary components.
- Carry out a partial implementation, using established bar code structures to identify whether they can be the basis of a resolution system. For example, the EPCglobal ONS system for serialised GTIN actually resolves on exactly the same code structure as the GS1 GTIN.
- Explore the development of various resolvers based on object identifiers and possibly other URN structures that can make use of data encoded in RFID tags.

While we consider that some of this research could be undertaken as part of the CASAGRAS project, this will still – of the nature agreed for that project – fall short of a proper pilot scheme.

9.2 Data exchange protocols

The current status of data exchange protocols is discussed in clause 7.12. Here we focus on some of the issues associated with converting a code into a format suitable for Internet communication using resolution services.

9.2.1 Future drivers

Resolution services will need to be developed around the object identifier structure, given that it is the basis of encoding data in ISO-compliant RFID systems. One challenge might be associated with the different number of arcs in object identifier structures from different domains. Alternatively, the concept of a root-OID might enable a simple resolver structure to be developed. This could also provide some elements of security and robustness, because some resolution services could be specific to one business / commercial domain. We would see further detailed research of OID-based resolvers being undertaken within the CASAGRAS project.

In our initial report (June 2008) we expressed some concern about a Standard from the ITU (Recommendation X.668) for a new object identifier structure aimed explicitly at RFID. Our concern then was that such a solution would be promoted to those organisations with either long namespaces or long unique item identifiers, creating conflict among user organisations that had long-established legacy data systems. We have since been in discussion with proposers of the scheme, and there is an understanding that the scheme will be offered as an alternative object identifier scheme, probably aimed at new applications. Therefore, the proposed short OID scheme needs to be properly integrated into the various object identifier structures that are being considered by user organisations for adopting RFID. The short OID (requiring at least two bytes) is no more efficient for encoding on the RFID than the established approach of encoding a long root-OID with a mechanism in the RFID data protocol that - irrespective of the length of the root-OID - only requires 5 bits or 13 bits on memory.

There is no doubt that one of the future drivers, in terms of accessing and exchanging information, will be the Object Name Service of EPCglobal. As the ONS is modelled on the prime Internet resolver, the Domain Name Service, its basic construction is sound.

Given that the structure of the Japanese Ubiquitous Code is not dissimilar, this too could be a major mechanism for accessing data to link objects to the internet. It is not clear what attitude the Japanese government and standards development organisations take with respect to the Ubiquitous Code. Over recent years, we have noticed that these formal organisations have sometimes distanced themselves from the code and at other times have promoted the Ubiquitous Code. It is still not clear how the Ubiquitous Code can be distinguished from other codes in the data carriers that can carry the code.

9.2.2 Constraints

Any of these object name resolution services either make use of the Internet itself or the physical infrastructure that supports the internet (e.g. Broadband access). Irrespective of whether access to the data behind a resolution service is free or paid for, the infrastructure itself could impose constraints in terms of the bandwidth available and the speed of access offered to end users. This might vary between countries, between regions, and between service providers. This is a factor that is already apparent with access to Broadband with the present Internet facilities being offered.

There have also been arguments associated with the future of the Internet that, irrespective of whether the world replaces copper wire with fibre optics, there is still a requirement to go through computer gateways. If the apparent "free-for-use" network is insufficient to meet the requirement for commercial look-up purposes, then the trade-off will either be lower service, or the need to provide a robust service for separate, paid-for, networks.

Similar constraints apply to data exchange as to pervasive networked systems (see 9.1.2): the competition for Internet services from increased legal and illegal traffic.

9.2.3 Comparisons and gap analysis

The introduction of the EPC code was heralded with the prospect of a simple unique item identifier code being all that was required, and everything else would be looked up on the Internet. A sideways comparison to the GS1 system at the point in time when the EPC system was being developed would have indicated an exactly opposite trend. Bar codes, and particularly 2D symbols, were increasingly being used in different sectors where information was critical for business purposes. The "micro-database" in a data carrier was used by transport companies to avoid look-up on fast-moving conveyor systems, by postal services to reduce the level of fraud from franked post and, more recently, with smart card by governments for biometrics passports.

We have already mentioned elsewhere in this report the fact that some applications that required UHF technology were constrained from adopting RFID because of a very narrow focus on unique item identifiers. The position is changing, and RFID tags of different frequencies are being offered with different amounts of memory. The encoding capacity on UHF tags seems to be increasing while, at the same time, new high frequency tags are entering the market with smaller encoding capacity. The fact that attribute data can be encoded on the RFID tag is a characteristic that will need to be taken into account in the development of data exchange protocols.

Local direct access from the data carrier, combined with essential look-up, might well be a future direction worth exploring. Also, the look up could be site-based offering greater security and a more consistent quality of service. A problem with a look-up system is that it only provides historical information; so, for example, it cannot provide information of a change of routing that can be written to a tag instantly, but has a lag effect of being added to any look-up system and made accessible to various partners. Furthermore, real point-of-time data such as that from sensors has to be based on the data carrier and can only be looked up once it becomes an historical record.

Significant further research is required to determine the dependencies and implications of critical failure so that a correct balance is struck between look-up via external data exchange protocols, via internal look-up facilities, and attribute data encoded on the RFID tag.

9.3 Privacy and security

We have discussed privacy and data protection in Clause 7.3 and security in Clause 7.13. As these topics are closely inter-related, we have decided to consider them together in this clause.

9.3.1 Future drivers

If we place aside some of the discussions that RFID is no different from any other data capture technique, there is still a public perception that the technology is different. Already, there has been legislation or guidelines to provide advice on the data protection aspects of RFID, and criminal laws defined in the United States against unauthorised reading of RFID tags to track and trace individuals without their consent.

As more and more applications become exposed to the general public, there is likely to be an increase in the lobbying for introducing privacy-enhancing technologies (PETs). The development of Near Field Communication and other mobile phone data capture, including the recent introduction of Touchatags, does bring about some potentially contrary attitudes. In the abstract, RFID can be considered the bête noire, but when some useful functions are offered to individual citizens, they may well literally buy-in to the technology. This has certainly been the case with both public and university libraries since the first library adopted RFID in 1998. Twenty-one years and 2500 libraries and half a billion tags later the citizens who use the technology like the technology.

As we have already discussed, such developments in lobbying might actually pose some threats to RFID systems where security is at a low level of implementation. So the combination, irrespective of whether the requirements are for the privacy of citizens or security of the application, means that there is a requirement for greater attention and technological solutions to be developed. Whether these address the needs of the privacy lobbyists or the security of business applications then becomes a moot point.

The initiative from the EU Commission for a Mandate that, inter alia, requests the European Standards Organizations work on standards aspects of RFID privacy and security is a step that should focus attention on this area.

9.3.2 Constraints

We have indicated elsewhere in this report that retro-engineering the design of RFID tags, in particular, is a difficult challenge. Any new security or privacy feature is likely to be considered by the standards bodies and technology vendors as an optional feature, because it is unlikely that everyone will agree that such a feature is essential for every application. It is also unlikely that vendors and end users will agree to implement any change that renders all existing devices obsolete either with immediate effect or within a limited time frame. Therefore, a realistic proposition is as follows:

- If any of the standards can be modified to accept privacy enhancing techniques or security features, then this needs to be done on an optional basis with existing standards. However, application standards, or even legislatures, could determine a "sunset" date for non-compliant technology to no longer be acceptable for specifically defined applications. Cognisance need to be taken of the replacement cycle of RFID tags, interrogators, and other devices. GS1 has worked on a 7-year sunset period for some aspects of its application. This might be reduced, but any period shorter than three years will be costly to existing users. A variation adopted by IATA for its *Simplifying the Business* programme, is to set two dates. Adapted for this purpose, all products and new implementations would be expected to support the new privacy and security by a given date and all prevailing applications expected to have fully converted at a slightly later date.

- As new air interface technologies are considered (and there are some currently work-in-progress), privacy and security features should be considered as an essential component of the scope of the standard.

9.3.3 Comparisons and gap analysis

There are many technologies that provide a greater threat to individual privacy than the RFID tag. Studies have shown that people who use Bluetooth linked to their mobile phones can be tracked using a computer. Research carried out by Vassilis Kostakos of the University of Bath (New Scientist 2008-05-07) during a six-month study in the city of Bath, identified approximately 10,000 unique devices. The researchers were able to track these devices within a 10 metre range whenever they were in the reading field. In a separate study the author has compared the threats of RFID and Bluetooth. His report concludes:

> "While RFID has captured the attention of both the research and consumer communities, Bluetooth has quietly become one of the most widely used technologies found on the streets today. In this article we described the remarkable similarities in the threats posed by RFID and Bluetooth. Furthermore, while a number of mechanisms have been developed to curb those threats in relation to RFID, few of these mechanisms transfer well to Bluetooth. In fact, Bluetooth's increased range and ease of scanning greatly increases those threats."

We draw this comparison, because few mechanisms are being implemented to reduce the privacy threats of Bluetooth.

Focusing more particularly on RFID, we identify two significant gaps, and therefore a requirement for education:

- The technologists have tended to pay little attention to privacy and security issues associated with RFID technology. In the past, they have been able to identify some of the privacy concerns as justifiably over-exaggerated, but have failed to address the negative impact of opinions, even if falsely based and lacking in understanding of the laws of physics. Probably, by bundling together issues of privacy and security and additionally taking into account the potential pervasiveness of mobile phone data capture, some serious education and then action could take place.
- Equally, legislators need to accept that there are serious constraints about retro-engineering some features to long-established technology. If rules in Europe are too stringent, what might happen is that the market might fragment with compliant and non-

compliant products. Unless a global, and equal, attitude is taken by all governments (which, with recent more serious financial issues has not manifested itself), there will always be the potential of less secure devices continuing to seep into the European marketplace. Therefore, a balance needs to be struck between making improvements for security and privacy, without killing off the market and the potential benefits of the Internet of Things. The approach taken by the legislators in Washington State USA strikes a reasonable chord. The intention is to make illegal any form of tracking of individuals using RFID, without imposing onerous cost burdens on the technology or banning it.

9.4 Intellectual Property issues

Given the technological nature of RFID, there are certain to be ongoing issues about IP in the standardisation field. We have recent experience of a novel idea being freely offered for a standard, while other committee members required that a statement be issued that there was no associated IP on the idea. Suspicion and opportunity seem to exist around every corner with RFID!

Most organisations apply an IP policy that at face value tends to equate to that of ISO being a Reasonable And Non-Discriminatory (RAND) IP policy. However there are detailed subtleties.

We raised the issue of IP in our June 2008 report, and now put forward a slightly different viewpoint, which is fundamentally based on the membership rules of organisations and issues that arise when cross-references are made between standards, each of which contains IP under different membership rules. We discuss this in more detail below.

9.4.1 Future drivers

A significant future driver will be the ongoing cross-referencing between standards developed by different organisations. For example, a number of ISO standards now make normative references of EPCglobal standards, Near Field Communication specifications make normative references to ISO standards, and so forth. This approach is necessary to reduce the development cycle and make use of significant technical expert resources that have built the original standard. So, in addition to one technology standard referring to another, ultimately application standards must make normative references to technology standards.

This gives rise to two quite significant secondary issues. As the market expands, there is no certainty – although custom and practice has so far been against this with AIDC technology – that the end user would be expected to license IP, other than the royalty payments between technology vendors being incorporated into the price of the product. It is unclear how this uncertainty can be eliminated or even reduced.

The other aspect is that if a particular application, or set of applications that use a particular RFID air interface protocol, are extremely successful, new technology vendors will enter the marketplace. Some of the historical statements about IP on the technology might no longer apply. Recently, the United States Department of Justice agreed not to oppose an agreement between seven companies to jointly license patents related to UHF RFID technology. As these patents applied to ISO/IEC 18000-6C and the EPCglobal Class 1 Generation 2 tags, it is clear that IP exists whatever claims are made.

Another major driver will be the development of new technology by different companies in the field of security, sensors, printed RFID and so forth. Some mechanism needs to be found for financially rewarding research and development producing good ideas that can be incorporated into standardised technology. This is to avoid future fragmentation of the marketplace, with proprietary components not being part of a standard, even as an optional feature.

9.4.2 Constraints

The issue that we are about to raise is not necessarily a constraint, but more a reality-based limiting factor. The standards-making process involves the participation of technical experts whose activity is determined by the membership rules of the standards-making organisations.

- For ISO, ISO/IEC and CEN standards, individual experts are selected and nominated by their National Standards Body to participate as individual experts to contribute to the process. Individual experts, irrespective of their eminence, can only participate as a member of a National Body or or Liaison Organisation. The net effect is that the pool of experts that participate in formal standards do not necessarily represent, either by employment status or national body affiliation, all the commercial interests in the development and resulting market opportunities. Some of the non-participants might well have relevant IP that impacts on a standard. Experts are expected to provide information about IP that might affect the standard, whether it is held by them individually, by their employers, or by others. Also, there is usually a call for IP to be declared against a standard, inviting any non-participant to make appropriate declarations.

- A second category of organisation is one that imposes an IP policy on all its corporate members, irrespective of whether they participate in the development of a particular standard or not. Usually, there are checks and balances before a standard is published, giving all members an opportunity to declare such IP. In the case of ETSI, if this IP is not offered on a fair, reasonable and non-discriminatory basis, the standard can be withdrawn with the experts tasked to re-write the standard avoiding the specific IP.

- The third category of memebrship is slightly more complex, because it uses membership of the particular committee drafting the standard as the prime domain for declaring IP. Such a process can identify IP at a very early stage among the activists drafting the standard, even leading to claims that a standard is IP-free.

There are different levels of complexity associated with each of the IP declaration policies. Assumptions cannot be made by any one organisation that the IP policy of another is identical. Equally, none of the standards-making organisations can provide a copper-bottom assurance of the IP status of any standard because non-participants might emerge some time later – typically when the market is large enough to exploit – and make retrospective claims on the implementation of the standard.

A third point is that technology providers who did not necessarily participate in the development process can only be assured that they need to address IP if it is declared in the standard. If there is an implication that the standard has no IP, but individual organisation or groups such as the RFID Consortium (the subject of the recent US DoJ court ruling) exists, then there is a known claim to IP. If such organisations do not exist, then the position is extremely uncertain.

9.4.3 Comparisons and gap analysis

We feel that it is relatively important to research and define the IP rules for various major standards-making organisations. We recommend that other parts of the GRIFS project undertake more detailed research to explore the situation when one standards-making organisation makes a normative reference to a standard published by another organisation. The additional research should also consider the implications of adding new features to the base standard.

We feel that the European Commission could consider, selectively, another approach for addressing IP. If any application is the subject of a Mandate or Directive, it would be useful to identify that IP on a FRAND basis is acceptable between technology providers to expand the market and to increase competitiveness. At the same time, it should also be made clear that end users, whether large corporations or individual citizens, could not be challenged for infringing IP. In other words, the results of research and development of a feature for an artefact justifies reward by agreement between technology providers, which obviously might have an impact on the price of the technology; but the end users themselves (in these special circumstances) should have a legal assurance of being free from being challenged.

9.5 Air Interface

Developments over the past few years have ensured that all the major frequencies are acceptable on a global basis. There are still permitted power differences at 13.56 MHz. The use of the UHF frequency has resulted in parts of the spectrum being specified as nationally or regionally acceptable at specific frequencies between 860 and 960 MHz. This is simply because of the lack of availability of a common range in the spectrum other than this 100 MHz band.

9.5.1 Future drivers

The recent auction of parts of the 700 MHz spectrum in the United States, possible because of the migration from analogue to digital television, sparked some interest in the United States about part of that spectrum being available for RFID. We have not noticed any major discussion about this within Europe. The last thing that is needed is for a completely new area of the spectrum to be exploited for RFID in one part of the world, with other regions not addressing the issues.

There needs to be ongoing development to achieve comparative performance capabilities, particularly within the UHF spectrum between different countries and radio regions. The proposals this year to relax the European listen-before-talk procedure has made a contribution, but there are still significant differences between the number of channels available in different parts of the world.

9.5.2 Constraints

If we focus on the UHF spectrum, then the biggest constraint – particularly for Europe – is the inability to match conformance and implementation features possible in the United States because of the significantly greater number of channels that are available.

9.5.3 Comparisons and gap analysis

There are still significant differences in the regulations that apply to RFID in different parts of the world. Europe is potentially in a strong position by having the political structure that could lead to common regulations across the European Union, and those regulations being applied simultaneously rather than waiting for national regulators to make the final decision.

Some experts have expressed concern that an on-going problem exists because different countries only use a small part of the spectrum within the 860 to 960 MHz range requiring compromises in tag design. The suggestion is that greater harmonisation can be achieved by migrating more regulations away from the extremes of this range. Other experts disagree and consider that the bandwidth for tag operation is not a real problem. In their view the focus should be on ensuring that different regulatory authorities provide additional bandwidth within their domain to enable more channels be used, and also to enable application is to adopt improved channel management techniques.

9.6 Sensors

We have already discussed sensors in clause 7.5, offering a narrow definition of sensors being attached to RFID tags and communicating by using the tag's air interface protocol.

9.6.1 Future Drivers

Three standards are close to finalisation, and they define the functionality of sensors for RFID. The IEEE 1451.7 standard specifies what some call "full function sensors", with the potential of sensing anything that can be measured and delivering some fairly complex records. The other is ISO/IEC 18000-6 that specifies simple sensors, which are intended to be embedded on the same silicon platform as the RFID chip. This results in significantly fewer types of sensors, and simpler metrics. In time, the expectation is that the simple sensor might be disposable and focused on major environmental attributes like temperature and humidity. The other standard is ISO/IEC 24753 that specifies the rules for interpreting the bits in the sensor memory into real numbers, and vice versa for configuring the sensor.

Although sensors for RFID exist in proprietary technologies, no artefacts have yet been built that are compliant to these standards. The same applies to support for sensors on the air interface protocol. So far, only two air interface protocol standards are being developed to support sensors: ISO/IEC 18000-6 Type C, which can support full function and simple sensors, and ISO/IEC 18000-6 Type which, by its nature, can only support simple sensors.

Initially, these standardised sensors are likely to address applications that already use proprietary technologies. This includes temperature control – particularly in the food supply chain – and humidity and shock in industrial supply chains.

A significant drive to open up the market will come if any major supply chain application decides that monitoring the environment is beneficial, or if a government authority decides that, for food or product safety, some form of monitoring is essential.

9.6.2 Constraints

The cost of RFID/sensor devices will be a major issue relative to their take-up. Some of the costs might be amortized if sensors can be re-used and re-configured a number of times during the life span of a single-use battery, or extended by using rechargeable batteries, or extended further (typically in more expensive sensors) by replacing batteries.

The security aspects of sensor data is critical, particularly if one of the purposes of sensors is to prove that a product is safe or to identify a point of time when safety or quality had been adversely affected. Because these are open standards, assured security is impossible but overall enhancements to RFID security, particularly on the write cycle, requires some serious consideration with respect to sensors.

9.6.3 Comparisons and gap analysis

A major gap also exists between the desirability to monitor items for safety purposes and any legal or commercially mandated framework that requires this. Adding sensors to prove the "safety" of a supply chain might bring kudos to an adopting organisation, but at cost. A Mandate can bring benefits to society.

The fundamental assumption of adding sensors to RFID is the dual benefit of capturing object-related data and environment-related data within the same data capture system. The premise is that adding functionality to RFID adds benefits. Other air interface protocols might well be developed that produce a lower cost sensor device, which would require separate interrogation processes to that of RFID. Already, GE Research has announced the development of certain chemical sensors as simple go/no go devices that make use of the antenna of RFID tags. Such sensors cannot offer the functionality of even a simple sensor, as currently defined, but might be sufficient to meet market needs.

An alternative at the other extreme is for more sophisticated sensors to be integrated, for example in containers that can monitor a defined space with more sensor probes and use completely conventional wireless communication with host systems.

9.7 Mobile phones

We have discussed mobile phones in clause 7.15, and it is clear that already there are independent and divergent activities taking place with respect to the choice of frequency, air interface protocol, and assumptions about what is encoded on the RFID tag.

9.7.1 Future Drivers

There is no doubt that major work will continue in the NFC Forum to push forward the 13.56 MHz technology, and the potential is for billions of mobile telephones to be RFID-enabled. Already, Alcatel-Lucent (an associate member of the NFC Forum) have launched Touchatags to address applications of benefit to consumers through to businesses.

The position with Korea requires further investigation, as Samsung and ETRI (the sponsors of much of the work in JTC1 SC31 WG6) are both members of the NFC Forum.

If RFID in the supply chain is to be linked to mobile phones, the major future driver will be the EPCglobal decision on which frequency and air interface protocol is mandated for use at item level coding. Currently, no decision has been made, and leaving the decision open-ended on the RFID side, combined with different approaches adopted on the mobile phone side of frequencies, does make for an uncertain future.

9.7.2 Constraints

The theme running through our discussions in clause 7.15 and above, is that there are far too many uncertainties and divergences in approach, both on the mobile phone side and on the RFID side. These are the major issues that we consider need to be addressed, and with some urgency:

- The NFC Forum has opted to support ISO/IEC 14443 air interface protocol, which is unlikely ever to be used for RFID for item management, but is suitable for electronic purposes and some of the target applications defined. Migration to ISO/IEC 18000-3 Mode 1 (equivalent of ISO/IEC 15693 for smart card) and to ISO/IEC 18000-3 Mode 3 (EPCglobal HF Gen 2) would result in a paradigm shift to link RFID for item management with a mobile phone.

- The differences between the work of JTC1 SC31 WG6 and the NFC Forum need to be addressed.

- EPCglobal needs to decide on a preferred frequency for RFID at the item level. If it chooses UHF technology, then there will be a significant gap between future developments in the NFC Forum and RFID for item management, which may have positive as well as negative implications.

- Whereas specific applications with the NFC Forum and in the standard being developed in JTC1 SC31 WG6 can support different types of encoding on the tag, greater cognisance needs to be taken of what is actually encoded on tags for RFID for item management.

9.7.3 Comparisons and gap analysis

If any of the constraints discussed above are not addressed, then **the prospect is for a set of standards that are fundamentally inoperable.**

In parallel to all of the work on RFID, it is possible to exploit the camera and screen display on a mobile phone to use existing, or new, bar code symbologies as a means of data capture. This technology is being considered both in SC31 WG6 activities and by the GS1 Mobile Communications group. By the very nature of the scope of its activities, it is not being considered by the Near Field Communication Forum.

Given the significantly greater number of mobile phones with camera and screen functions over those with RFID, this is an area that is worth considering. In addition, as we discussed in 9.1, there is an already established infrastructure for bar codes in place, some of which encode data that is already in a structure that can be presented in a URN format.

9.8 Hybrid technologies

The general definition of a hybrid technology could be the combination of any pair (or more) of data capture technologies. For the purpose of this report, our focus is on combinations of bar code and RFID. Obvious examples exist where permanently encoded bar codes and RFID can be combined, e.g. in Driver Licenses and what is being called "slap and ship" labels to meet the mandate requirements of retailers adopting EPCglobal standards.

The constraining feature of this hybrid approach is that the bar code remains permanently encoded and, in supply chain situations, often renders the RFID tag as a single trip disposable item. New technology from Japan has resulted in rewritable media that can completely change bar code and other eye readable media. This is currently being standardised as ISO/IEC 29133 *Information technology – Automatic identification and data capture techniques – Quality test specification for Rewritable Hybrid Media data carriers.* The final ballot to approve publication is currently taking place.

Japanese industry intends to use the technology as part of its successful KANBAN (just-in-time) manufacturing system to replace single-use cards, and introduce RFID at the same time. The current state of the technology is based effectively on contact erasing and printing of the optically readable data, but research is ongoing to be able to erase and rewrite at distances comparable with the read and write range of 13.56 MHz.

9.8.1 Future Drivers

As is typical of developments of technology in Japan, the proposals for standardisation of this technology were only submitted to ISO after the technology had been researched and developed, with support from Japanese government funding. Therefore, there is no doubt that applications will be developed in Japan, and possibly applied in Japanese-owned manufacturing plants around the world.

The contact printing technology aspect, on its own, is already in daily use in Japan in mass transit systems, but the major point from an RFID perspective is that, by encoding complementary data on the RFID tag, a number of applications will be able to implement RFID systems with the knowledge that the tag can be re-used a number of times, when combined with the rewritable bar code. This will not suit all applications, but Japanese industry is certainly seeing this as a means of accelerating the take-up and minimising some of the migration problems from bar code to RFID.

Other applications for rewritable hybrid media include the introduction of sensors to the RFID component. Again, the re-use aspect can have a significant benefit in the introduction of the technology.

Because of the data on the RFID tag and on the bar code can be complementary, there are various combinations that can be applied. If the technology was used in applications that did involve personal data, then the bar code component could provide a better means of ensuring privacy than the RFID tag.

9.8.2 Constraints

Probably the biggest constraint with the technology would be the "not invented here" syndrome of potential users in the West. There is also the potential technology push problem from Japanese vendors, who might consider that the national marketplace (whether B2B or B2C) can be replicated on a worldwide basis.

Another constraint might be simply one of perception of the technologies. There are still very few vendors that have an in-depth understanding of bar code and RFID, and those that do often have to decide on the basis of an OR logic the merits of one technology over another when developing a solution for a customer. Hybrid Media adds a new paradigm that requires some education and the possibility of applying an AND logic.

9.8.3 Comparisons and gap analysis

To some extent, we have touched on the gap analysis immediately above. There will certainly be many instances where simply retaining bar code in an application without adding RFID will remain a major cost driver, irrespective of the benefits of adding RFID. Such applications are either when the bar code has a short ephemeral life span or has a long life span, with few – but intermittent – data capture requirements.

In a similar manner, there will be applications where RFID will, of its own accord, replace or provide functionality that cannot be addressed by bar code.

The potential for using rewritable hybrid media requires some further research, probably undertaken by the commercial organisations interested in exploiting the technology. Additionally some form of education is then required in the sectors where the technology can provide clear benefits and accelerate the take-up of RFID.

9.9 EU Harmonisation

We have discussed in clause 7.11 some of the environmental issues and Directives where RFID may make a contribution to the process. What we would like to discuss here, is the positive contribution that the EU Commission can make with respect to RFID technology.

9.9.1 Future Drivers

Many of the Directives that require some form of track and trace or identification make very few specific requirements on how this is to be implemented. This appears to be in sharper contrast to the prospect of requiring specific implementation to meet privacy requirements. Given that problems in some traceability systems lead to death, injury or serious illness, society is faced with some challenges. There are various requirements for traceability of food stuffs, pharmaceuticals and critical safety components for air transportation that are either the subject of Directives and/or standards supported by EU Mandates. Some specify bar code data capture, some make no specific recommendations about automatic identification capture, and none – to our knowledge – specify RFID.

There are sectors that are not necessarily covered by existing Directives that also present opportunities. The Commission's EU RFID Expert Group had been advised that a significant number of deaths and injury could be reduced in hospitals by adopting RFID and AIDC technologies. A standardisation proposal to track and trace safety-critical automotive parts in a similar manner to the processes applied to aircraft safety-critical parts has been submitted to the European Commission by CEN/TC 225. Given the number of European citizens that die in air crashes, compared to those that die in hospitals or road accidents, opportunities exist both to promote the take-up of technology, and to bring potential benefits to society.

In addition to the prospects of adding more implementation requirements to existing Directives, and to develop new Directives that are associated with the health and safety of citizens, the Commission has an interest in promoting the Internet of Things. It can take a number of attitudes ranging from a *laissez faire* one of letting it happen, or using its various mechanisms to achieve solutions that work in a particular direction. In the latter case, it has issued a Mandate including standardization on privacy and security for RFID, which is open-ended enough to encourage innovation, yet achieve the overall goal of filling existing gaps. The *laissez faire* approach, with respect to what has happened with mobile telephones and RFID, is an indication that there is a risk of significant levels of interoperability between systems that have millions – if not billions – of Euro investment behind them.

9.9.2 Constraints

Although the European Union is potentially the most significant economic unit in the world, it requires to operate globally with many other economically powerful nations and regions. A balance needs to be struck between the benefits and costs of applying any mechanisms that place constraints on RFID implementations that are not applied in other parts of the world. This might apply to requirements for privacy and security that are not necessarily supported globally. Therefore, any feature that adds costs to European businesses without bringing the benefits of similar businesses in other parts of the world might even result in inertia in the take-up of the technology within Europe.

Promoting aspects of the technology within Europe, as suggested above for various traceability projects, also has to be handled very carefully. For example, adding costs to the automotive sector for tracing safety critical parts for sale in Europe could make the industry less competitive than in other regions. Finding a balance that provides benefits to the industry too, or some mechanism that makes the economics of the solution viable, can help.

We have no detailed views on how these conundrums should be tackled, other than pointing out that they require some very serious consideration.

9.9.3 Comparisons and gap analysis

There is certainly an opportunity to develop a high level, strategic blueprint for the direction that RFID should take in Europe to bring benefits to businesses and society. We do not see such a blueprint as being fixed in time, but continually reviewed. Then, that blueprint can be matched against developments taking place in other regions and an ongoing comparison and gap analysis should take place, possibly with input from experts.

Our research has identified a number of developments either in regions or by commercial organisations that need serious consideration. We cite a few as examples below:

- The approach to tracking and tracing of private individuals with RFID has been addressed in an interesting manner by the new law in Washington State USA. By making the activity a criminal offence, the cost burden to industry is minimised, but most of the privacy concerns are addressed.

- The Japanese approach for addressing RFID as a technology that might potentially cause problems for citizens having electronic medical devices brings an obvious benefit to society.

- The speculation in the United States about using 700 MHz frequency for RFID requires further research.

- The Japanese development of rewritable hybrid media needs to be considered as a technology, and with some implications for privacy and security.

- The significant per capita investment by Korea in RFID compared to any other country requires analysis, and not necessarily the equivalent Euro levels of investment.

Above all, anything that the Commission undertakes has to be based on factual analysis, with avoidance of marketplace hype, and even over-egging issues by lobbyists and research organisations.

10 Conclusions and recommendations

10.1 Conclusions

10.1.1 The role of the European Commission

It is clear from the Commission's support for the GRIFS project, for the CASAGRAS project, and a number of other projects with an RFID theme, that it sees long term benefits in the take-up of RFID within Europe. Although the GRIFS project has an international flavour, the funding and initial initiative has come from Europe. In clause 9.9, we suggested that a high level strategic blueprint for the development of RFID should be in place and continually reviewed. Such a blueprint would also be a focus for ongoing activities once the Global RFID Standards Forum is established.

At the moment, a significant amount of standards development is taking place on the basis of commercial decisions of stakeholders: the user community seeking some new feature or the vendor community offering a product or development to gain market acceptance through the kudos of a standard. The decision about agreeing to work on a new standard or enhancing an existing one often fails to take account the potential development of the technology in the round**.** As an example of this has there been integration of developments of Near Field Communication and the introduction of ISO/IEC 18000-3 Mode 3, for either standards-making community?

A European RFID roadmap might contribute to a better understanding of the steps and progress necessary to co-ordinate activities. The Commission has expressed a view that a future lies with the Internet of Things. We use the Internet of Things as an example, but there are probably a number of areas where the Commission has a vision of the future. The vision is clear, how to get there is obscure. Some standards that are being developed will probably make little or no contribution to the goal, but be justified for other purposes. Some requirements to meet the vision might not even be addressed by the current standards work programmes. An RFID roadmap defined by the Commission and developed in conjunction with European experts would provide a sound basis for creating some type of scorecard of areas of standardisation that the European Commission considered of benefit to European businesses and citizens. Such an approach would still enable completely independent developments in the standards-making world, but the focus on a realistic master plan would provide some stability for the future direction of the European industry.

The approach would have another advantage, in that it would require the various policy-making Directorates General to identify the role that the technology could play within their scope of policy making. Given the RFID initiative by DG Information Society and Media, there is already a platform for cross-fertilisation. If such an approach was adopted, it would be significantly different from initiatives taken in other parts of the world where specific targets (e.g. Homeland Security in the United States) or support for research organisations (e.g. ETRI in Korea) have been the focus of government support for the technology.

10.1.2 Preparing and maintaining the standards map

The prime task assigned to us in Work Package 1 of the GRIFS project was to prepare a standards map and provide supportive analysis. During our research, we have found that access to information is variable, including some significant differences even between different ISO committees. The quality of the information can certainly improve with insider knowledge that is not generally available to the public. As the authors have insider knowledge for some areas, and are members of the public for others, this is reflected in the quality of our analysis.

Even during the research period, the position that we started with at the beginning, and what has been included in the report, has changed. A few standards have been published, some have moved on to the next stage having reached some approval milestone, others have been delayed because additional research and development are required to move them forward, and there have been new projects approved and other projects submitted for approval. There have even been changes in committee structures.

It is clear that if our work is not continually updated, it will gradually deteriorate in quality with the passage of time. Although the intention is to update the work towards the end of the GRIFS project, **this probably loses a valuable resource.** Some thought needs to be given to ongoing updates of the status of standards.

While we recognise that this is a valuable resource, we also advise against making it too easy to copy. The risk is that some unauthorised organisation might take all the data, publish it, and cause confusion in the marketplace. To this end, we are pleased that our original recommendation of having something like a managed wiki, where changes can only be made under editorial control, has been achieved in the development of the **GRIFS RFID Standards Database**. Individual information can easily be copied, but the mass copying of the resource will prove difficult and infringe copyright.

The architectural model in Clause 1.2.1 was developed retrospectively by creating it from component parts in Clause 7. It is clear that an RFID system from tag to resolver has essential complex components. As yet, not all these components are in place, but the time is probably right not only for the ongoing work with the GRIFS project to co-ordinate activities, but also to provide ongoing status reports and associated educational material.

10.1.3 The implications of many overlapping initiatives

Our research has identified a number of areas where different organisations are involved with the same technology, overlapping aspects of the technology, or related functions. In particular, we cite:

- 13.56 MHz technology which is used for smart card, RFID for item management and for mobile phones by the Near Field Communication Forum.

- Activity on mobile phones is, itself, also diverse with the NFC Forum focusing on 13.56 MHz technology, JTC1 SC31 WG6 focusing more on UHF technology and bar code. The GS1 Mobile Communications group has been established to look at some of the technology and application areas. Not only are the fundamental technology issues different, but there is also evidence of a significant difference in the approach to what is encoded on the RFID tag, and how it is processed to provide services to the users.

- There has also been a degree of overlapping with respect to solutions for namespaces for unique identifiers, with work from ITU-T that differs from that of JTC1 SC31 and EPCglobal.

- Similar points can be made with respect to developments that will lead to the Internet of Things, that need to involve some of the organisations mentioned above, plus the Internet Engineering Task Force and the European Commission itself.

- Finally, on this list of overlaps is the issue of privacy and security associated with RFID. There have been tendencies for security standards to be developed in splendid isolation of a holistic approach to the technology. We expect the work carried out in response to the new EU Mandate to try to co-ordinate the more relevant components.

To assist with identifying relationships with RFID, we have produced a first version model of a network of influencing developments (see 1.2.2). We do not claim that this model is fully comprehensive. It certainly does imply the need for a significantly greater amount of co-ordination not just at the higher "management level" of standards-making, but at the coal face where experts from different disciplinary backgrounds need to understand the issues that impact on others.

10.1.4 Project Development Cycles

In our report in June 2008, we gave some examples of work that was taking place in one arena that could have an impact on another. The fundamental situation has not changed, and there is still a significant lack of understanding of what is going on, even in the next sub-group, let alone what is going on between fundamentally differently structured standards-making organisations and stakeholders. A new example that we can cite is all the new work item proposals for mobile phone standards in JTC1 SC31. A number of the proposals were crafted without a detailed understanding of other activities within that AIDC standards committee, and certainly without taking into account activities within the Near Field Communication Forum. However, rather than criticise the authors of these proposals, we could equally raise questions about some of the finished work of the NFC Forum itself. No one group can necessarily claim comprehensive understanding of relevant standards developments that are taking place elsewhere that will impact on the group's work developing RFID standards. The result is the probable fragmentation and duplication of some activities.

We consider that a first step before any new standards project is proposed is that reference is made to a resource such as the GRIFS RFID Standards Database**.** In addition a call should be made among the stakeholders for a network of experts to be established who are able to communicate with one another to clarify issues. This will certainly make it significantly easier to reference other standards-makers' documents on a technical basis. Certainly, one of the first steps to achieving this would be to clearly define objectives and scopes of all the standards and specifications on the database. Currently, such information is a bit patchwork, even from the same source. The ISO website sometimes provides an abstract of the scope of a standard, but for other ISO standards there is often little more than the title of the standard and the last recorded stage of work. We do not see any advantage in simply linking web-sites. These are often governed by strict access permissions applied to the entire standards organisation. If the GRIFS project is to succeed it must draw its information from formal sources (such as the official websites) and informal sources (such as the experts working in the area, but who have no control of the formal sources).

We do not see any realistic prospect of shortening any of the standards-making process stages, as discussed in Clause 4. We consider that there should be a greater focus on the exchange of information between experts from different standards-making domains to ensure that the development process – both in draft standards and in the review process - has the potential to achieve a higher quality of content. Therefore it is recommended that standards organisations be informed in an early stage of each other's standardisation projects in order to build effective liaisons between each other's experts.

Given a typical three-year elapsed time, some specific initiatives are required to keep experts in the different standards-making communities up-to-date with developments outside their specific domain. As an example a six-monthly updated business plan at the JTC1 Sub Committee Work Group level and made publicly available could be a step forward for GRIFS to address. We conclude that improved awareness and communication between experts is a significant requirement to be addressed in the Memorandum of Understanding.

10.1.5 Intellectual Property and standards bodies

The detailed procedures for declaring IP, and the scope of their impact, varies according to the membership rules of the different standards-making bodies. We accept the rules as given, but draw attention to the fact that there are implications for different classes of technology vendor, depending on their level of participation in the standard. In clause 9.4, we suggest an approach that the European Commission could take for any mandated application. This recognises the justification in applying FRAND principles for IP, but proposes some legal framework to ensure that EU support for the technology does not result in either vendors or end users being exploited. As we have no legal expertise, we are sure that if the idea is taken up that a legal framework would be established to ensure a level playing field in the roll-out of RFID for any Commission-sponsored application.

10.1.6 Data protection, privacy regulations and security

There have been a number of proposals, particularly from an academic base, to introduce privacy enhancing techniques (PETs) to RFID technology. Few, almost none, of such PETs are so far present in the devices and the air interface protocol standards.

It is far easier, and probably more effective, to impose constraints on what data may be encoded in an RFID tag. To comply with the data protection requirements, the basic advice that should be adopted by any application standard is to encode the minimum, or no, personal data. Most RFID technology will be associated with item-related data and not personal data, in sharp contrast to the smart card. For most applications, there is little need for any form of personal data to be encoded on the RFID tag.

Although it is theoretically possible for anyone to access a data base or data exchange system (like the EPCglobal ONS) on the basic product identification, most general enquiries from citizens will probably only return details such as the product description. In other words, without levels of permission - **that are part of the database security not the RFID technology itself** - access to personal data from RFID tags can be difficult, or made to be difficult by invoking basic data protection principles and processes.

There is no doubt that PETs will be developed and will be implemented in RFID technology. A serious problem is that the existing RFID technology is being implemented on a daily basis, increasing the size and value of the infrastructure and providing inertia to any form of switch-over. At some point in the future, the scale of the problem will be similar to changing the size of railway track gauges, or changing roads and vehicles so that all countries drive on the same side. A closer reference can be made to the fact that retail bar code scanning is using a 35-year-old technology. It has not been significantly upgraded despite lots of opportunities to introduce technical advances, it certainly has not been replaced and RFID is the first new technology to be proposed to operate in parallel. New bar code symbologies (data carriers) are being introduced, but usually with a 5 to 7 year phased introduction.

If PETs are introduced as options in the RFID technologies, then requirements for their use might be specified for particular applications. In these circumstances take-up can be accelerated. However, applying them to general item level coding for retail products is an extremely difficult challenge to implement, even within the European Union, given the global trade implications.

With respect to security, there is certainly an element of overlapping between standards-making activities. One way that this could be better coordinated is to involve as part of the GRIFS project those organisations that claim to have security standards for RFID. This is certainly an initiative that is worth exploring.

Probably of greatest significance from a European perspective, is the Mandate from the European Commission, which requires due account to be taken of standards issues on privacy and security. The very nature of this Mandate requires a number of different threads to be pulled together, for formal recommendations to be made to the Commission and approved for the development of specific standards dealing with RFID technology.

10.1.7 Air interface issues

There are still some significant performance differences from using the same air interface protocol in different radio regions. A major concern for Europe has been removed by no longer requiring the listen-before-talk procedure for UHF systems. There is still the issue between the regions of differences in the number of channels that can be used within the UHF spectrum. While it is probably impossible to extend the number of channels in Europe to be comparable with that of the United States, anything that can be done through the efforts of ETSI and the radio regulators to improve performance capabilities is welcomed.

We identified sources from the United States about the auction of spectrum in the region of 700 MHz because of the migration of television broadcasting from analogue to digital. Some experts in the United States considered this to be the "next big thing" for RFID. We have seen little discussion of this in Europe, but the matter needs to be addressed to ensure long term alignment.

10.1.8 Conformance and performance standards

Both the EPCglobal and US Department of Defense initiatives suggest that developing some kind of certification programme is desirable and possible in the early days of the deployment of the technology. A bigger challenge exists with a long-established technology such as the 18000-3 Mode 1 air interface protocol where, because of its link with smart card, there is an estimated 1 million readers already deployed. However, even with this technology as true open system application standards are developed (e.g. in this particular ISO 28560 for RFID for libraries) then interoperability becomes an issue if users are to gain all the benefits of open systems. We conclude that as interoperability becomes a reality, that greater emphasis will need to be placed on application-centred certification.

10.1.9 Data standards

The ISO RFID data standards depend on an object identifier structure to provide a namespace identifier for the unique item identifier, and also to identify additional object-related data (e.g. batch, expiry, destination). This structure provides the uniqueness and persistence that is required for resolving over the Internet. Because it is registration requirement of the Registration Authority for ISO/IEC 15961-2, the OID structure can provide ongoing support for either new RFID applications, or legacy applications migrating to RFID. Similarly, the Registration Authority for ISO/IEC 15459 offers opportunities for extending the capability of traceability systems, supporting any form of legacy code structure.

There is certainly a requirement for increasing awareness of user groups to the functions and processes of these Registration Authorities. Consideration should be given to at least some form of pan-European promotion and publicity to increase understanding of the Registration Authorities among the user sectors. This might be a specific task to be undertaken by CEN.

10.1.10 Data encoding and protocol standards

There are indications of an even greater misunderstanding about RFID among those responsible for developing application standards. To cite a real example, one organisation assumed that data could be encoded to their own encoding rules yet be compliant and that there were no technology constraints in reading data across the air interface and therefore there was no need for efficient encoding. To date, applications to the Registration Authority for ISO/IEC 15961-2 indicate that some organisations are unaware of the different air interface protocols, that RFID data encoding and communications are different from bar codes, and that it is possible to selectively read and write and modify data. An implication of this is that assumptions are made that bar code encoding rules can simply be applied to RFID. Because user organisations generally interface with vendors, who are not necessarily aware of all the standards issues, this can further contribute to a lack of user understanding. There is a requirement to provide educational and support information to help user bodies understand the standardisation issues. This is particularly the case where the application calls for complex sets of data to be encoded.

10.1.11 Application standards

We were able to identify a limited number of RFID application standards, but could find few details of others where we understood that an RFID application existed. In clause 7.10, we identified some communication gaps, both from the vendor community and the user community. Some vendors had misunderstood the requirements for encoded data for some of the applications, and the user community often does not have sufficient understanding of the technology and certainly the inter-relationship of standards.

We mentioned above the possibility of CEN reaching out to the user community with respect to creating an understanding about object identifiers. Probably an even greater task is one to ensure that basic information is available to the user community about the current status of RFID standards.

We are undecided about whether user organisations responsible for developing application standards should be formally part of the GRIFS structure, or involved at some associate level.

10.1.12 The Internet of Things

Besides the ongoing development of the EPCglobal ONS system, there is still significant scope for resolving other types of URN over the Internet. We recognise that the major thrust of such research is to be undertaken within the CASAGRAS project. What is essential within the GRIFS project is to ensure that various applications that will require or benefit from participating in the Internet of Things have an early understanding of the issues. The focus needs to be on the different user sectors that would typically qualify as a liaison member of a CEN or ISO committee. To this extent, we conclude that this is another dimension of extending support to those organisations developing application standards for RFID. As above, the European domain could be addressed by CEN.

10.1.13 Data exchange standards and protocols

It is generally acknowledged that the EPC structure lends itself, through the ONS system, to be resolved over the Internet, but the Internet supports a number of URN structures including object identifiers. A problem remains with the OID structure, which is that different domains (namespaces) use different structures and hierarchical levels to identify a unique item. We anticipate that additional research might be undertaken within the CASAGRAS project to clarify whether the concept of a root-OID can be used within the resolver services.

10.1.14 Device interface standards

A real challenge exists in whether it is possible to develop device interface standards retrospectively for long-established air interface protocols operating in some frequencies. One method that can be considered is to take a different approach, and not necessarily standardise the interface, but "expose" interfaces with the components that would otherwise sit at either end of a device interface standard. There have already been developments in this direction, particularly from RFID printer encoder manufacturers. In addition to supporting their proprietary encoding language and protocols, some provide an additional interface by exposing XML interfaces. If a software application above the interrogator is also XML-enabled, then it is possible to develop specific interfaces between the components. Although this is not necessarily as "standardised" as a device interface standard, it certainly improves the opportunity for cross-collaboration in a manner that is significantly simpler than having to address the detailed proprietary interrogator programming language and protocol.

10.1.15 Mobile phones and RFID

Although the capability of mobile phones being used for data capture purposes has little direct impact on RFID for supply chains, it could be a significant long term driver for the take-up of the technology and acceptance by ordinary citizens. Therefore, there is a need to ensure that there is greater alignment between the activities of the Near Field Communications Forum, JTC1 SC31 WG6 and the general direction of RFID in the supply chain. The NFC Forum should be a key target to be part of the Memorandum of Understanding.

10.1.16 Health and Safety regulations

Logically, both the Health and Safety requirements discussed in clause 7.2 need to be incorporated into the RFID air interface conformance standards. This is certainly a position that has been recognised by JTC1 SC31 – at least in principle. The real challenge is that conformance standards are focused exclusively on air interface conformance. The impact on the human body in terms of a SAR value (Specific Energy Absorption Rate) depends very much on the design and manufacture of an interrogator. Therefore, this calls for type testing of devices rather than just a mention in the generic air interface conformance standard.

A major problem still exists with respect to potential interference between RFID devices and electronic medical devices that are implanted or carried by the patient. Generally speaking, such medical devices are designed and tested against a set of likely devices that might interfere, but as new technology such as RFID is introduced and enhanced, electronic medical devices cannot be expected to have in-built features that deal with this new potential interference. From discussions during the ISO committee meetings with the regulators and manufacturers of such medical devices, it is clear that the onus of non-interference is expected to rest with the manufacturers of RFID devices. Few procedures are in place to ensure this.

10.1.17 Sensors

Probably by 2010, RFID tags that support sensors in a manner compliant with associated standards can be expected in the market place. This will open up a number of potential applications both with respect to food traceability, and other critical items that can be damaged by a change in environment.

An issue (see our Conclusion on application standards above) is that this functionality needs to be understood by various organisations involved in the supply chain.

10.2 Justification for an RFID MoU

The report gives an overview of the various standards making bodies involved in the preparation of standards for the various components of the RFID model. Given the interrelationship between these components, it becomes clear that co-ordination between the various standards making bodies is of the utmost importance. A Memorandum of Understanding (MoU) between the various standards making bodies could meet this need for co-ordination. An example for the creation of such a MoU could be the MoU on electronic business between ISO, IEC and ITU.

One of the important tasks of the RFID MoU would be the (decentralised) maintenance of the database with RFID standards. The maintenance of this database would allow the identification of potential overlap between standards and the identification of new standardisation areas. A major benefit would be that stakeholders not directly involved in standardisation would have a complete and up-to-date overview of all relevant RFID standards.

10.3 GRIFS Co-ordination targets

It is surprising how many organisations seem to be represented in activities associated with RFID. If we start with the core area of RFID for item management at JTC1 SC31 WG4, we feel that there is a requirement for more co-ordination between this group and two other working groups of JTC1 SC31:

- WG5 Real Time Locating Systems

- WG6 Mobile Item Identification and Management (MIIM)

Widening the circle, the following technology standards-making organisations need to be taken into consideration for co-ordination:

- JTC1 SC17 Identification Cards
- EPCglobal
- ETSI TC ERM: EMC and Radio Spectrum Matters
- ETSI TC TISPAN: Telecomms and Internet Converge Services and Protocols for Advanced Networks
- CEN TC225 AIDC Technologies
- ITU-T (and/or JTC1 SC6 Telecommunications and Information Exchange Between Systems)
- Near Field Communication Forum
- Internet Engineering Task Force
- IEEE Standards Association – Instrumentation and Measurement (for sensors)
- GS1 Mobile Communications Group

Among the application areas, co-ordination could take place with:

- ISO TC104 Freight Containers
- ISO TC122 Packaging and Joint Working Group on Supply Chain Applications
- ISO TC204 Intelligent Transport System
- ISO TC46 SC4 Information and documentation, Technical interoperability
- For air transportation: IATA and ATA
- For the automotive industry: AIAG, ODETTE, JAMA, and STAR
- Other potential application developers as appropriate

The following groups need to be taken into account:

- The European Commission, particularly DG Information Society and Media
- CENELEC TC106X Electromagnetic fields in the human environment