Collaborative Project

ASPIRE

Advanced Sensors and lightweight Programmable middleware for Innovative Rfid Enterprise applications

FP7 Contract: ICT-*215417*-CP

WP2 – Requirements and Specifications

Public report - Deliverable

D2.5 - Privacy Specifications

Due date of deliverable:	M6
Actual Submission date:	M6

Deliverable ID:	**WP2/D2.5**
Deliverable Title:	**Privacy Specifications**
Responsible partner:	OSI – Open Source Innovation Ltd
Contributors:	Aalborg University
Estimated Indicative Person Months:	8

Start Date of the Project: 1 January 2008 Duration: 36 Months

Revision: V5.0
Dissemination Level: PU (public))

Document Information

Document Name: **D2.5 – Privacy Specifications**
Document ID: **WP2/D2.5**
Revision: **V5.0**
Revision Date: **13-June-2008**
Author: **Humberto Morán**
Security: **none (public document)**

Approvals

	Name	Organization	Date	Visa
Coordinator	Neeli Rashmi Prasad	CTIF-AAU		
Technical Coordinator	John Soldatos and Albena Mihovska	AIT and CTIF-AAU		
Quality Manager	Thomas Christiansen	CTIF-AAU		

Document history

Revision	Date	Modification	Authors
V0	13/03/08	Creation of outline	Humberto Morán
V1	10/04/08	First draft of the document	Humberto Morán
V1.1	15/04/08	Proof reading of first draft	Alexandra Komissarova Dominika Kwasnicka
V2	23/05/08	Addition of content	Mathieu David
V3	13/05/08	Addition of content	Humberto Morán
V3.1	06/06/08	Review and Addition of content	Ramiro Samano Robles
V3.2	12/06/08	Review and Addition of content	Puri Novelti Anggraeni
V3.3	12/06/08	Review	Peter Denton
V4	13/06/08	Consolidation of Review Input	Humberto Morán
V5	13/06/08	Addition of Section 3 Final review	Humberto Morán Dominika Kwasnicka

Content

Section 1 Executive summary

ASPIRE is a breakthrough project in RFID as it is the only middleware that currently considers privacy by design and by default, while incorporating and enforcing regulatory principles in its design and implementation.

Privacy threats from breakthrough information technologies are becoming a "hot topic" as privacy violations are soaring – e.g. as with The Internet. For example, Google has been recently given a warning by the European Commission related to the privacy violations associated with the storage of searches made by its users; and Facebook was also given a warning because this company was illicitly retaining personal data even after the closure of user accounts.

Due to the rapid evolution and widespread adoption of highly sophisticated, pervasive and connected information and communication technologies (ICT) the right to privacy, hitherto taken for granted, is rapidly and unnoticeably eroding and threatening society as we know it. The erosion of privacy and intrusion by ICT is also source of many novel and increasingly frequent abuses. Illicit practices such as identity theft, phishing, pharming, spamming, spyware and computer viruses thrive in and further contribute to the erosion of privacy, and are at the centre of a new type of organised crime, or the cyber-crime.

In the case of RFID, privacy is an important topic because this technology has the potential to change the privacy landscape of industry and consumers. Whilst The Internet provides users with a default "opt-out option" (e.g. no one is forced to go online or provide any personal data); RFID tags placed on everyday objects will seamlessly infiltrate society in an unprecedented way, and so generate scores of data about objects and their owners and carriers. For instance, most existing passive RFID tags (tags which draw their power from the interrogation field and hence do not require batteries) cannot easily support encryption and authentication engines so the most common ones can be freely read by any compatible reader. Furthermore, the tag identity in the numbering scheme of some leading RFID standards reveals information about the product type and product item. Consequently, third parties such as snoopers, thieves and terrorists are able to detect and abuse tags on objects carried by common citizens.

Privacy and security issues are not limited to consumers: RFID tags in products can be abused before the point of sale (POS) for industrial espionage (e.g. by surveying competitor's products in a shared transport system or warehouse; or by detecting and tracking confidential products); can be abused by counterfeiters (e.g. by cloning or transplanting them); or can be abused by unscrupulous retailers (e.g. engaging into consumer profiling or registering consumer behaviour without consent).

Although some solutions to the "promiscuity" of existing passive RFID tags have been proposed, these are not considered satisfactory by regulators, privacy advocates and consumer associations. For instance, the "killing" or removal of tags at the point of sale is unreliable, cannot be easily automated, and prevents a number of valuable applications. Similarly, password-protected RFID tags still pose tremendous technical challenges and are not suitable for most RFID item-level applications. For this reason, regulators and legislators are in urgent need of guaranteeing that industry, citizens and especially consumers are protected against privacy threats from RFID.

ASPIRE is not impervious to these issues and so was devised to protect the privacy and security of end users and consumers. Whilst the ASPIRE project does not intend to solve all RFID-related privacy and security issues, it focuses on protecting privacy before the

point of sale, specifically by addressing the possibility of establishing and abusing the relationship between object and personal data by ASPIRE adopters and their business partners; and by protecting not only personal data but also object data, and so hindering the possibility of industrial misuse of tags. More specifically, ASPIRE addresses these privacy and security issues by:

- Incorporating the e-Privacy Directive in its design and development. This involves the translation of the directive in specific technical specifications such as data structures and algorithms (e.g. algorithms which purposely break the relationship between object and personal data; and algorithms that "clean" unnecessary data).
- Incorporating advanced mechanisms for the secure collection, storage and transmission of data. Among other measures, this includes secure protocols and algorithms for the secure collection and transmission of RFID and personal data; use of secure databases (e.g. with encryption mechanisms); and the separation of backups to allow for the selective deletion of personal data which is not longer required.
- Developing and disseminating best practices for the collection and management of RFID and personal data. This includes business and operational processes.
- Creating certification and auditing programmes and privacy seals to guarantee the correct implementation and use of ASPIRE and so enforce its privacy and security measures.
- Engaging in dissemination to promote consumer awareness so as to allow consumers to exert the right to choose privacy-friendly suppliers as advertised by ASPIRE's privacy seals.
- Making its source code available to the community of RFID stakeholders by using open source software, and so allowing for maximum transparency in the implementation and enforcement of privacy and assuring consumers that their privacy is protected.

We recognise that ASPIRE does not solve all privacy and security issues related to RFID. For example, post-POS abuses of tags are not fully addressed by ASPIRE as these challenges require safer, so far inexistent, passive tags. However, our approach is a very important first step in addressing a growing threat for society and industry, that of compromised security and privacy resulting from the widespread adoption of intrusive and pervasive ICT.

1.1 Contents and purpose

The present document examines and details all necessary specifications for the protection of consumer and end-user privacy and security in the context of ASPIRE. The purpose is to establish the Privacy Specifications for our design, development and implementation activities with the aim to maximise the social acceptability of the final ASPIRE middleware.

Specifically, this document analyses end-user requirements, social and legal background, state of the art and other RFID dimensions conditioning the privacy characteristics of the ASPIRE platform; and proposes specific design, development and implementation approaches to ensure the protection of industry and consumer privacy. The aim is to ensure that such data as behavioural or personal data is treated accordingly to the principles established in the e-Privacy Directive (data quality, conservation and limitation) and other related European directives and legislation. This treatment of the data is not limited to technical specifications, but extends to the necessary specifications and best practices to allow the creation and execution of a certification programme and associated privacy seals for ASPIRE adopters.

Section 1 (this section) elaborates on the executive summary, document contents, state of the art and innovation brought. It also justifies deviations from the original objectives (none in our case) and establishes the intellectual property approach for the document.

Section 2 elaborates on the conceptual and contextual elements of RFID privacy, state of the art, and position of RFID stakeholders. Specifically, it reviews on RFID privacy and security issues, position of the different RFID stakeholders, possible solutions to its privacy and security issues, legal background in Europe such as the e-Privacy Directive, and the specific focus of ASPIRE.

Section 3 summarises and analyses the impact of end-user requirements on RFID privacy and security, specifically drawing from an online survey performed by the ASPIRE Consortium in the Member States of its partners (Portugal, Greece, United Kingdom, France and Denmark).

Section 4 explains the fundamentals by which ASPIRE aims to protect privacy and security of industry and consumers. These are: (a) transparency (ASPIRE middleware has "nothing to hide" and our privacy and security approaches are open to public scrutiny); (b) consumer education, in order to make informed decisions as to their rights and possibilities to privacy and security; (c) auditing and certification, in order to guarantee that ASPIRE adopters do not fraudulently modify the middleware and follow the privacy and security recommendations made by ASPIRE; and (d) incorporation of the principles of the e-Privacy Directive in ASPIRE's design (data structures and algorithms).

Section 5 elaborates on the importance of transparency, highlighting the advantages of open source software and documentation over proprietary RFID solutions. It explains that some important privacy threats take place at software level so it is at this level that these should be addressed. It also discusses alternatives for auditing and certifying open source software despite the fact that it can be fraudulently or accidentally modified by some adopters.

Section 6 discusses the importance of consumer education, particularly that related to

privacy and security threats from RFID; and ASPIRE's advantages and limitations in this sense. It draws from existing RFID surveys and research at European level, and from the ASPIRE survey. The purpose is to identify priorities for consumer education and propose alternatives to engage into proper and targeted dissemination of ASPIRE and its advantages for consumers.

Section 7 details alternatives and proposes options for the auditing of the privacy-friendly ASPIRE middleware; the creation of certification programmes to differentiate those adopters who successfully implement and follow ASPIRE's privacy and security recommendations; and the creation of privacy seals to provide consumers with the right to choose providers where privacy and security are ensured by means of ASPIRE.

Section 8 elaborates on privacy-friendly algorithms and best practices that reflect the e-Privacy Directive in the design, development and implementation of ASPIRE.

This document concludes with a section that summarises the privacy approach of ASPIRE, its advantages and limitations, and possibilities for future research. Whilst we acknowledge that ASPIRE does not solve all privacy challenges facing RFID, we also believe that our project is a very important first step to protect industry and consumers from the threats of pervasive technologies. With ASPIRE, our Consortium expects to set a trend with the potential of changing the privacy landscape of ICT (Aspire today, inspire tomorrow). For this, further research on ICT-related RFID privacy and security (outside the scope of ASPIRE) is proposed at the end of this document.

1.2 Brief description of the state of the art and the innovation brought

RFID is recognised by many experts as the "next big thing in information and communication technologies" after The Internet because it allows bridging the virtual and physical worlds and offers tremendous economic, social and environmental benefits resulting from an improved traceability of products, raw material and equipment. For instance, in 2005 the United Nation's ITU predicted "The Internet of Things" and highlighted its world-changing potential, benefits and perils[1]. In their opinion, the impact of "The Internet of Things" will be many times greater than that of The Internet. Many other technology think-tanks have also put their bets on the side of RFID.

RFID is a very simple but promising technology: it consists on tiny (and relatively inexpensive) devices connected to an antenna in order to wirelessly send and receive data to other similar devices or specialised interrogators or "readers". In its most basic version, the only data received and transmitted by these devices is an identity, which in some numbering schemes (standards) are unique. This allows using RFID devices as "electronic tags" to identify and locate everyday objects. Furthermore, the so called "passive" RFID tags draw their operational power through electromagnetic induction from the interrogator's signal, hence rendering batteries unnecessary and so offer a long life and very low manufacturing and operational costs. Conversely, the so called "active" tags incorporate a battery that increases their processing power and communication range; and can therefore store data "in the tag" and incorporate security functions (encryption, authentication etc.) and sensors to monitor environmental conditions (temperature, humidity etc.).

Industrial uses of RFID are countless, in particular for retailers, distributors and manufacturers. Among many other valuable applications, the so-called electronic barcodes can help to fight counterfeiting and shoplifting; streamline product recalls,

inventory visibility and on-shelf availability; control storage conditions; increase consumer value from better and fresher products; enhance product manufacturing, checkouts and returns; monitor livestock for the prevention of diseases; improve lifestyle from domestic applications; and support packaging recycling and reusing.

This potential has led industry, academics, governments and standardisation bodies to heavily invest in the improvement, standardisation, dissemination and adoption of RFID technology. One recent development worth mentioning is the Auto-ID Project, an American initiative led by industry and academia which rapidly spread to the rest of the world, aiming at the improvement and standardisation of RFID in the tagging of Fast Moving Consumer Goods (FMCG) as a replacement of the aged barcode. Partners of the 1999-2003 project included leading retailers, manufacturers, technology vendors and research centres such as Wal-Mart, Metro, Gillette, Procter and Gamble, Unilever, Nestlé, Tesco, UPC/EAN, IBM, Philips, SAP and the MIT. The partnership rapidly grew to more than 800 organisations and research centres around the world, and evolved into the ongoing EPCglobal/GS1.

However, many experts now recognise that RFID has not lived up to expectations. In 2006 the European Commission held a Europe-wide RFID consultation that revealed the controversial nature of this technology[2]. An article by The Economist shows that the market for RFID has grown well below forecast and that there are still many challenges facing the widespread adoption of this technology[3]. Among these challenges can be highlighted privacy and security issues, incompatible standards and frequency regulations, limited reliability when used on metals or liquids, and the lack of a clear business case for many applications due to high operating and/or implementation costs (cost of ownership). RFID is an immature technology with many opportunities for improvement, and ASPIRE is addressing many of these.

In particular, RFID has been subject to strong criticism by privacy advocates, consumer associations, governments and regulators; and even by extreme religious groups. Its usual privacy and security fears include Orwellian practices by governments and industry, and the exposure of citizens to snooping and theft by third parties – e.g. when carrying expensive or sensitive objects tagged with RFID. Whilst it is clear that some of these fears are unfounded and rather paranoid – e.g. those based on conspiracy theories; it is also true that some others are very reasonable and well founded – e.g. those related to the abuse of insecure tags by third parties such as snoopers, thieves or terrorists. For this reason, RFID promoters are proposing the removal or disabling (killing) of tags at the point of sale (POS). However, these approaches prevent many valuable applications such as after sales services, are unreliable, and require extra action by consumers – privacy and security is not their "default" behaviour. More specifically, it is feared that children, the elderly and technology-unaware citizens will fail to protect themselves from the perils of this technology. For this reason, privacy advocates and regulators are not convinced and the debate on privacy and security issues around RFID is still ongoing.

Importantly, RFID is different from such previous ICT as The Internet and its applications because of its tremendous potential for seamless intrusiveness, first and foremost when passive RFID tags are used to identify products in the supermarket as these products will be purchased by people who may have never heard about RFID and its privacy and security threats.

ASPIRE is innovative because it is the first RFID middleware to incorporate specific mechanisms to protect privacy, specifically by implementing the e-Privacy Directive and other related principles in its developments by means of privacy-friendly and security-friendly algorithms. Hitherto and despite the fact that many privacy threats take place at

software level, all RFID software developments have overlooked privacy and security issues. For instance, many important privacy threats for consumers result from the possibility of mixing personal and object data (who bought or wears certain products). For example, a supermarket can register the identity of objects bought by specific customers who are identified by their credit or loyalty cards. This information can be used later to: (a) identify the whereabouts of customers by tracing the detection of tags on their property in other places – e.g. other shops in the chain; (b) identify and profile consumers when they come back to the retail shop; and (c) be sold to centralised databases where a whole "picture" of the consumer and his or her shopping habits is built. This is especially relevant in objects that can be used as "identity proxies" such as shoes, clothing, personal medicines or medical implants.

Similarly, information about privacy-sensitive or security-sensitive products tagged with RFID should be properly protected. For example, the identity and data associated with tags located on embarrassing products such as adult nappies or medicines for embarrassing or sensitive diseases should be kept secure; and so should be the identity and data associated with expensive products such as jewellery or consumer electronics.

The position of the different RFID stakeholders varies from strong support to strong opposition. For instance, most technology vendors and some end-users have so far neglected the risks of RFID and emphasised the need of "consumer education" as a way of allaying fears[4]. As their understanding of the technology has increased, most privacy advocates and consumer associations have moved from strong opposition to reasonable opposition as they have understood that not all RFID applications and technologies pose privacy or security risks. Governments and regulators have actively promoted legal, regulatory and technological solutions to the RFID challenge, with the European Commission at the leading edge of the social acceptability of RFID after holding two consultations on the technology and funding research on its general impact.

However, industry and several governments (with the notable exception of the European Commission) seem to have overlooked the importance of contributing to the social maturity of RFID by promoting and funding further research on legal and regulatory aspects, and on Privacy Enhancing Technologies (PETs). The highly innovative ASPIRE shows the strong commitment by the European Commission to the finding of solutions that improve the social acceptability of RFID without hindering its tremendous economic advantages.

The debate as to the suitability and applicability of existing legislation to the case of RFID is also still ongoing. For instance, by the time this document was written the European Commission was finishing a public online consultation on RFID and privacy, and proposing recommendations in this sense. Particularly, stakeholders are considering whether the existing e-Privacy Directive suffices for RFID, or whether further legislation is required. This document addresses the issue of suitability and applicability of the e-Privacy Directive, and includes preliminary recommendations by the ASPIRE Consortium in this sense, and on the potential need for further legislation. These recommendations can be summarised as: (a) the e-Privacy Directive suffices to regulate the collection, processing and storage of RFID data BEFORE THE POINT OF SALE; and (b) the e-Privacy Directive is NOT SUFFICIENT to regulate privacy and security threats from RFID AFTER THE POINT OF SALE.

1.3 Deviation from objectives

This deliverable does not have significant deviations in respect to the original content. However, the legal and regulatory aspects required the incorporation of ongoing developments, especifically those related to the online consultation on RFID privacy held by the European Commission. Fortunately, these developments have not changed the ASPIRE landscape and context, which is privacy-friendly and secure by design and by default. Conversely, they have shown the vision and corporate responsibility of ASPIRE's partners, who addressed RFID privacy and security issues well before other RFID innovators took action on them.

In brief, this deliverable had to be extended in scope and content to incorporate important RFID developments in Europe, yet the original ASPIRE concept and objectives remain the same.

1.4 If relevant: corrective actions

Since there are no deviations from the original objectives, but rather an extension of scope and content, no corrective actions needed to be taken.

1.5 Intellectual Property Rights (IPR)

This document belongs to Open Source Innovation Ltd and the ASPIRE Consortium. These organisations have decided to make this document publicly available for the public benefit, under a General Public License (GPL)[5].

Open Source Innovation Ltd is a Charity registered in England, number 1110906. The publication of this document follows its Charitable Objects aiming at "the education of the general public in the field of Open Source Software", and "the promotion of OSS for the benefit of society and the environment".

Section 2 Background

2.1 Conception of RFID – why is it so different?

This section deals with the conception of RFID and its main differences from other wireless technologies.

Wireless technologies have existed for many years. For instance, analogue technologies such as the TV and the radio have been around for a long time. More recently, advances in digital technologies and miniaturisation; and the upsurge of computers, mobile phones and The Internet have led a revolution in which wireless devices have penetrated society to an extent never seen before.

For this reason, many RFID promoters compare this technology with other existing wireless devices (especially laptops and mobile phones). The argument is held that since these technologies have not eroded privacy and security to an unacceptable level, there is no need to be concerned about RFID and its privacy and security perils. In this argument, RFID is seen as a mere quantitative evolution of existing ubiquitous wireless devices; meaning cheaper, smaller and simpler.

However, we sustain that RFID does not only constitute a quantitative step relative to existing wireless technologies: it rather constitutes a qualitative step with a dramatic impact on society, environment and industry; and in particular on privacy and security of industry and consumers. To prove this hypothesis we need to further our understanding of the existing RFID technologies by addressing their conception, specific characteristics and their implications, as follows.

Conception – What is RFID?

One of the difficulties studying and dealing with this revolutionary technology is that the term "RFID" describes several types of tiny wireless technologies. Moreover, the usually referred taxonomy of "passive", "semi-active" and "active" tags is good for technical purposes yet inadequate to support its socio-technological study because it is too general (e.g. there are many types of passive tags) and refers to technical characteristics (e.g. does it have a battery?) rather than to functional characteristics (is it secure?). For this reason and to support this analysis, we propose a different taxonomy that furthers technical characteristics and maps these into functional characteristics. This taxonomy allows a better comparison of RFID with other wireless devices, and the correct analysis of its socio-technological process. The following table crosses the main technical characteristics of RFID with its functional characteristics:

1. Countless business, lifestyle and environmental benefits (strong benefits): as mentioned before, RFID has the potential to (a) transform the discrete supply chain by bringing tremendous operational improvements and cost efficiencies; (b) support domestic and lifestyle applications by allowing citizens to interact with their property; and (c) bring environmental benefits by saving energy, reducing consumption of raw material, and supporting recycling and reuse of packaging. For this reason, RFID is worth promoting and pursuing.
2. Significant network externalities (strong standardisation): for RFID to bring the aforementioned benefits across the supply chain and beyond there is a need for standardisation at many different levels, from air interfaces, to numbering schemes, to processing and exchanging data, to business processes. For this reason, RFID is worth standardising with open standards and converting into a

commodity.

3. Generates scores of id and other data (scores of data): RFID tags transmit their identity and/or data whenever and wherever they are placed within the reading range of a compatible reader, up to many times per second. Since it is foreseen that with the upsurge of The Internet of Things there will be many compatible RFID readers and several RFID tags around, the amount of data generated by RFID will be without precedent in the world of wireless technologies.
4. Functionality beyond control by the carrier (uncontrolled functionality): one of the remarkable characteristics of RFID in comparison with other wireless devices is that most RFID tags, particularly those passive tags currently proposed for the identification of Fast Moving Consumer Goods (FMCG), incorporate functionality that cannot be controlled by the carrier. For instance, these tags will reply with their unique identity when placed in the interrogation field of any compatible reader.
5. Small, quiet and seamless (unnoticeable): the functionality of RFID tags cannot be directly perceived by carriers as they do not emit any light nor produce any noise when interrogated. Moreover, some tags are so small that carriers may not even notice them.
6. Inexpensive and ubiquitous (cheap and pervasive): since these tags are very inexpensive and will be placed in equally inexpensive common objects such as FMCG, RFID has the potential to be the most pervasive wireless devices ever.

Figure 1 summarises the main functional characteristics that define RFID:

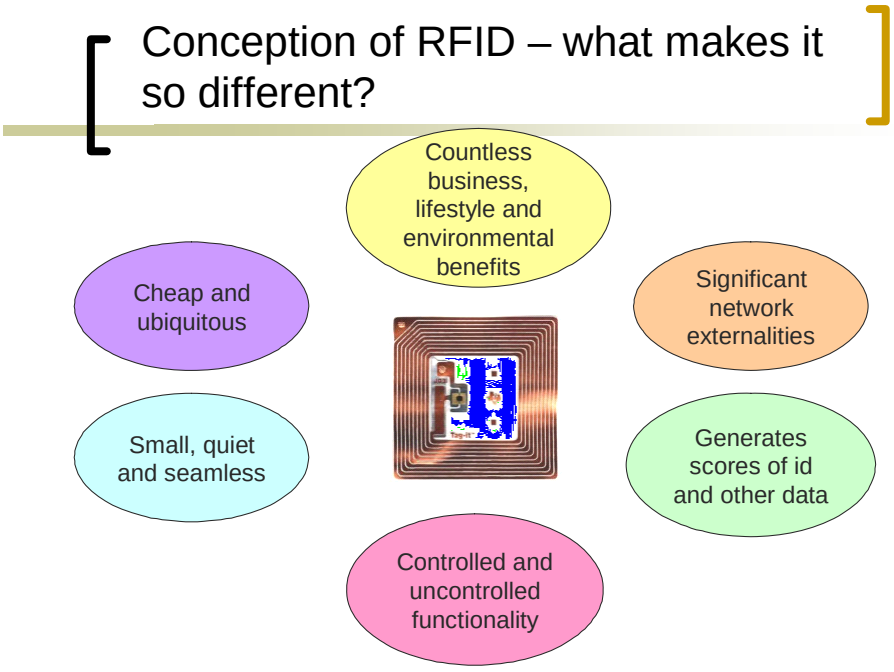

Figure 1: main functional characteristics that define RFID

To sum up, from a functional perspective RFID tags (in particular the passive identification tags) are wireless devices with tremendous potential benefits, strong standardisation requiring openness, that generate scores of data, which incorporate uncontrolled functionality, and that are unnoticeable and pervasive. This means that they will be everywhere and seamlessly talking in a common language (standard) to many similarly ubiquitous compatible readers and generating scores of transactions about us and our objects. Consequently, it is clear that their social impact is predicted enormous,

notably their potential to invade the public and domestic environments and pose noteworthy privacy and security threats.

How does RFID compare with other wireless technologies?

The following table compares some of the existing RFID devices and other wireless devices in the light of the aforementioned functional characteristics[6]:

Wireless device	Strong benefits	Strong standards	Scores of data	Uncontrolled functionality	Seamless	Cheap and pervasive
Passive RFID identification tags	Yes	Yes	Yes	Yes – tags need "killing" after the POS	Yes	Yes
Passive RFID identification tags with password (new devices by Alien Technologies)	Yes	No – password distribution is unsolved	Yes	Yes – unless tags are assigned a password	Yes	Yes – but less than those without password
Active RFID identification tags with password security	No – too expensive for most applications	No – password distribution is unsolved	Yes	No	Yes	No – too expensive for FMCG
Mobile phones (GSM)	Yes – as phones	Yes	Yes – voice	No – can be switched off	No – noises & lights	Yes – but much less than RFID
Wireless laptops	Yes – as laptops	Yes	Yes – data	No – full control	No – noises etc.	Not cheap, moderately pervasive
Blue Tooth devices	Yes – as extension devices	Yes	No	No – password is always required	No – blue light available	Yes – but much less than RFID
Zigbee devices	Yes – as wireless sensors	Yes	No	No – password is always required	In some cases	Moderately

Table 1: comparison of RFID and other wireless technologies

The previous table shows that RFID tags with no password protection are the cheapest and simplest to operate as they do not need password distribution mechanisms, and have the potential to become the most ubiquitous wireless devices ever. However, these are also the ones with all the highest potential to pose privacy and security issues because the combination of all these quantitative characteristics give place to a qualitative step relative to other wireless devices: they are everywhere seamlessly talking to everyone in a common language.

From all these functional characteristics, the one that mostly differentiates RFID from other wireless technologies from a privacy and security perspective is the "uncontrolled functionality". This is also the one that worries consumers the most, as some surveys have recently showed.

Why does RFID pose so many social challenges?

RFID poses significant social challenges because of its functional characteristics as explained before, and because of the complexity of its conception and variety of sub-technologies, alternatives and applications. For instance, there are many RFID applications such as pallet- and case-level tagging that do not pose any privacy or security threats to consumers. The item level tagging of such short-lived, inexpensive

and privacy-insensitive products as a can of soda does not pose significant privacy or security issues. Similarly, there are more sophisticated tags such as active tags with encryption and authentication mechanisms that do not pose privacy and security issues to carriers, yet these are unsuitable for most FMCG applications because of their high cost. Finally, industry and many RFID promoters have assumed that the killing or removal of the tag at the point of sale is a solution good enough to justify the roll-out of item-level tagging without concerns about consumer privacy and security. Further and more detailed examination by experts, privacy advocates and consumer associations proved that tag removal or killing is a bad solution which creates other issues and does not address all aspects of the privacy problem such the abuse of tags before the point of sale as proposed by ASPIRE.

RFID is neither a good nor a bad technology. This definition comprises a set of similar novel technologies and standards which are in process of maturing and have not been fully understood by stakeholders (from technology vendors to regulators). For this reason, the social impact of RFID is difficult to understand, anticipate and manage. With RFID, the devil is in the detail.

As we have seen, the social acceptability of some proposed RFID applications, especially those related to the item-level tagging of FMCG, is controversial. This suggest that some of the current RFID technologies are immature and not ready for social deployment, hence requiring further research not only from the technical perspective (e.g. PETs), but also from the socio-technological and legal perspectives. ASPIRE intends to address these issues by developing a privacy-friendly RFID middleware, which classifies as a Privacy Enhancing Technology or PET. It also intends to develop guidelines and a certification programme for the adoption and use of RFID, which classifies as socio-technological research.

What other challenges are facing RFID?

Privacy and security are not the only challenges facing the RFID revolution. As mentioned before in the quote by The Economist, standardisation and viability of business cases are also very critical.

Standardisation is essential in the case of RFID because most supply chain applications require tags to operate inter-organisationally, and require supply chain partners to exchange object information. Standardisation of RFID must take place at many different levels, from air interface (frequency, protocols etc.), to numbering schemes (to have a unique way of identifying objects), to reader interface (for interoperability and compatibility reasons), to data interface (to exchange object data), to business practices (e.g. in the placement of tags). The current RFID landscape is plagued with different standards, being the most relevant EPCglobal and ISO. Importantly and because RFID is a global technology (due to the globalisation of the supply chain), standardisation of RFID poses tremendous challenges in terms of governance. For instance, the country that controls the global RFID network will control the global supply chain. Due to security and sovereignty issues, the global RFID network needs to be governed by multiple countries in a way similar to The Internet.

The viability of business cases is also very important for the RFID revolution. At the moment, Moore's law has not worked in the case of RFID and the cost of tags and readers are stubbornly high. Some RFID think-tanks such as IDTechEx have expressed concerns about silicon RFID tags being able to cross the U$ 5 cent barrier ever, which is considered essential for the tipping of item-level tagging[7]. Importantly, SMEs have been sidelined in the RFID process because of the high cost of sensors, readers and

middleware. As the supply chain is mostly made of SMEs, this cost barrier is hindering this promising revolution.

Figure 2 summarises the socio-technological landscape of RFID, and links challenges, stakeholders and some potential solutions:

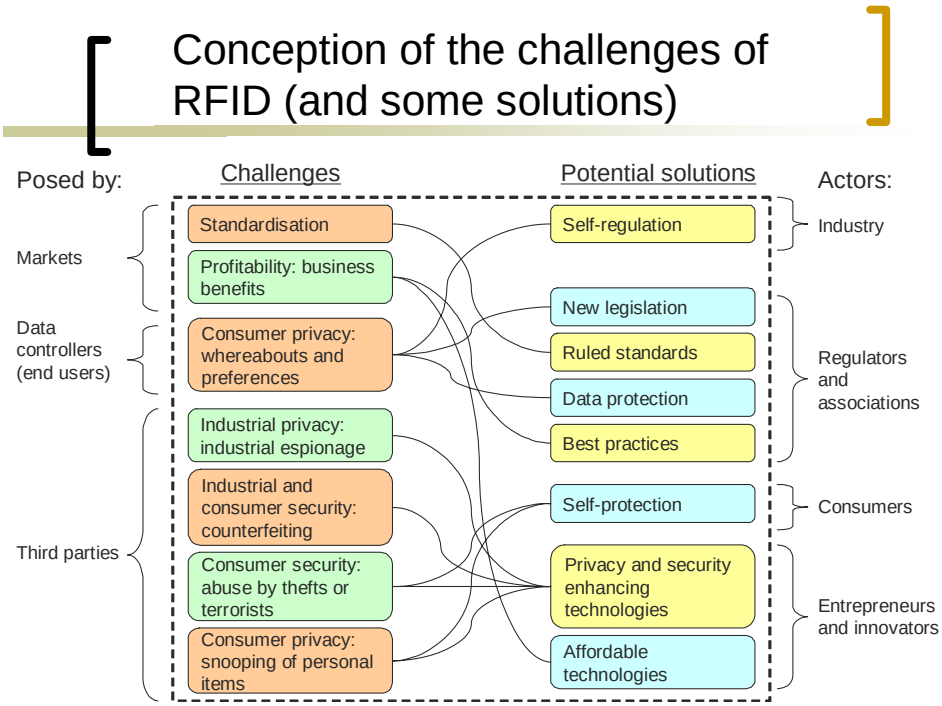

Figure 2: conception of the challenges of RFID (and some solutions)

ASPIRE will address some of these challenges by:

1. Implementing interoperability with existing standards at the level of data interfaces, in particular EPCglobal and ISO.
2. Providing the possibility of extension to new RFID standards by publishing its software and documentation under an open source license so new standard bodies and technology vendors have the possibility to incorporate the extensions.
3. Creating low-cost hardware (sensors and readers).
4. Creating a royalty-free open source RFID middleware tailored to European SMEs.
5. Targeting and involving SMEs in the ASPIRE project to incorporate their requirements and promote adoption and dissemination.

Of course, ASPIRE is not in a position to address such issues as the governance of the RFID network or the standardisation of frequencies at international level.

2.2 Privacy threats and other vulnerabilities of RFID systems

In wireless communications, the security aspect has always been a big issue. Maintaining the confidentiality and the integrity of the data is a main concern as people expect to send information only to targeted authority. With the development of the RFID Technology, a new kind of threat appears; the privacy threat. Privacy has become one of the most sensitive topics, since it has to deal not only with the privacy and integrity of

the company but also with the privacy of the consumer, who is the end-user in the production chain. These privacy threats become a reality as passive RFID tags are more and more implemented on everyday products – for example in Japan, more than 50 millions of RFID-enabled cell phones have been sold during the last year, allowing users to pay in more than 50,000 points of sale[8] – but even more because the RFID readers are small[9], relatively inexpensive, and have sufficient processing capabilities to read most of the tags.

These privacy and security risks are not limited to passive tags used for item-level tagging. Many other RFID devices, including active tags with no security or authentication or with lose security – e.g. a short password, can also be abused by suppliers or third parties. In particular, devices with memory used to store personal or confidential data may be abused by unscrupulous parties, for example by eavesdropping or fraudulently reading or modifying tag data. Similarly, devices with encryption or authentication have vulnerabilities and therefore cannot offer full protection to carriers. A list of these vulnerabilities follows:

Unauthorised reading or writing of tags: this, the simplest and more dangerous type of attack, consists of fraudulently accessing the information in the tag by either reading or modifying it. This is possible because many RFID tags (particularly the cheaper ones) lack security and hence can be read or written by any compatible reader. Other more sophisticated tags have encryption and/or authentication mechanisms to deal with unauthorised reads and writes. For example, in some authentication mechanisms the authenticating party generates a random key (challenge) to which a common function (not known by the attacker) is applied by both parties, and then compare results. The use of encryption requires a common public key, or a private key which can be established at object, product type or supplier level. However, the distribution of this key poses tremendous technical challenges, and its accidental disclosure may compromise the security of the entire RFID system.

Eavesdropping: using compatible reading devices, eavesdroppers can listen to the wireless communication between tags and readers, and so copy the information being transmitted in either direction. Depending on the RFID application, this information may include sensitive personal or object data, and hence give place to the privacy and security threats described above. In some cases, the eavesdropping device may even capture communications from a distance longer than the reading range of the RFID system being attacked. A potential counteractive measure for eavesdropping is to encrypt the message using strong encryption. However, the intrinsic simplicity and power limitation of existing passive and semi-passive tags (tags that use a battery to support functions other than wireless communication) mean that strong encryption is not possible in these cases, or it is too costly in terms of tag price or performance (speed and range). Tracking is another impact of eavesdropping. Simply encrypting the message or having pseudonym is not enough to prevent tag tracking.

Man-in-the-middle attack: this is a sophisticated attack in which a device acts as "intermediary" and pretends to be the reader to the tag; and the tag to the reader. In this case, the attacker can not only eavesdrop whilst transmitting the original information (also known as "relay attack"), but also purposely change the message for its advantage. Again, strong encryption is a good countermeasure for this kind of attack; whist authentication is not as reliable as the intermediary device can transmit the authenticating keys between both sides without interpreting them.

Physical and technical cloning: since insecure tags can be read without authorisation, these can be "duplicated" or "cloned" by creating one or more physically

and/or functionally identical tags. For example, counterfeiters can not only copy the original product, but also its tag. A special variation of cloning is the "functional cloning", in which the communication tag-reader is eavesdropped and then used to simulate either component ("reply attack").

Denial of service, or "jamming": RFID systems are especially vulnerable to interferences, in particular to intentional interferences. The "jamming" of the frequency by issuing a strong signal at the same frequency or artificially simulating the reply of thousands of tags with a special device (blocker device) has the potential to bring down any RFID system.

Malware or viruses: some RFID devices are known to be vulnerable to "viruses", similarly to any other computer. These can change the behaviour of the tag or the backend system and distort the information it contains or its identity. The virus can spread through the tag itself or through the backend system.

The main victims of insecure RFID are industry and consumers, although other end-users or carriers such as governments and employees respectively are also at risk. Privacy and security issues associated with RFID significantly differ before and after the point of sale (POS). This is mostly because after the POS RFID tags can be associated with consumers, whilst before the POS they only relate to products and companies. For this reason, our analysis is divided to pre-POS and post-POS (impact on industry and consumers, respectively).

Before the POS, the unauthorised detection of tags can be abused by third parties (thieves, counterfeiters and competitors) to engage in fraudulent practices. For example, thieves may detect valuable goods by scanning their RFID tags through packaging or even thin walls; counterfeiters can read tags on genuine products and so clone or transplant them on counterfeit; and competitors can spy on stock content and/or rotation level by scanning products in shared warehouses or distribution systems.

After the POS, if tags are not deactivated or removed, the authorised detection of tags can be abused by such third parties as thieves, snoopers or terrorists; or even by the product seller or associated service provider. Specifically:

- Thieves may detect valuable goods carried by consumers and rob them. Examples of these valuable goods are jewellery and consumers electronics.
- Snoopers may learn of consumer whereabouts or detect "embarrassing" or "private" products such as medicines, medical implants or political, religious or sexual objects. Typical examples include medicines for health conditions and adult nappies.
- Terrorists may detect and abuse sensitive political or religious objects such as religious or controversial books – e.g. a book by Salman Rushdie, The Old Testament etc.
- Retailers may engage in consumer profiling, discrimination, selective pricing, interactive undesired marketing, or collection of behavioural data. For example, they may be able to detect goods previously acquired in their own shops or from the competition, and estimate the value of the carried goods and therefore the affluence of each consumer.

As explained before, ASPIRE does not solve all privacy and security issues around RFID, its focus being the pre-POS and institutional abuse of the technology. The following table summarises privacy and security issues around item-level RFID, both before and

after the point of sale, and their relationship with ASPIRE – which addresses the impacts highlighted in red:

Nature of abuse	Privacy impact	Security impact
Before the POS		
Tag detection by thieves		Theft affecting industry
Tag detection by counterfeiters		Cloning or transplanting of the tag to counterfeit
Tag detection by competitors	Industrial espionage	Destruction of stock
After the point of sale		
Tag detection by snoopers and linkage with personal data	Whereabouts of consumers	
Tag detection by snoopers when it is located in privacy-sensitive products (e.g. medicines, embarrassing objects, implants, or religious, political or sexual objects)	Detection of privacy-sensitive products, embarrassment, discrimination.	
Tag detection by thieves when it is located in expensive products (e.g. jewellery)		Theft affecting consumers
Tag detection by terrorists when it is located in security-sensitive products (e.g. books on politics or religion; or police equipment)		Terrorism affecting consumers

Table 2: privacy and security issues around item-level RFID

In particular, privacy threats are more difficult to understand and show many ramifications[10], among which we can highlight:

The Action Threat:

In this threat, the behaviour or intent of a user can be inferred from the evolution of the group of tags surrounding him. For example, if you can read that someone has a two tickets for a football match for the Euro competition as well as airplane tickets in his suitcase, you can easily guess where this person will go in a near future. However, the match tickets can also be a gift for someone else and the plane tickets for a different purpose.

Association Threat:

In this threat, the consumer is directly connected to the product he owns. Not only the kind of products he owns, but the precise product he has can be discovered. For example, you can see someone listening to an MP3 player in the street, and you wouldn't have pay so much attention to it if you did not know that this precise MP3 player was one of 5 of a very special edition. Imagine what would happen if someone ill-intentioned had this RFID.

Location Threat:

In this threat, the location of someone can be revealed by the tags he is wearing. Since most of the readers are fixed, it can be quite easy to monitor someone's location through the whole day by checking all the places where some of the tags he is wearing have been read. Combining the location and time information, you could be able to draw his trajectory during the day and enter his own privacy and intimacy.

Preference Threat:

This threat is related to the specific kind of product someone owns and buys, to define his consumer profile and thus target him more specifically. For example, everything you buy in your usual supermarket could be stored in a profile linked to your credit card and so to your identity. Those profiles could then be used by the supermarket to send you targeted advertising and worst, to sell it to third companies that would in turn target you

with their specific products.

Constellation Threat:

The constellation threat is highly related to the location threat the difference being that it is not a targeted individual that is tracked but a random individual without knowing its identity. The tracking of this person would be performed by tracking the constellation of RFID tags that he is wearing. As an example, it can be used in a supermarket to monitor the flow of consumers, detects the area less attractive, and redesign the supermarket in consequences, or highlight specific products at the most popular places.

Transaction Threat:

In this threat, the tracking of goods does not stop at the consumer step, but goes further and keep on tracking the location and ownership of the tagged object through its entire product life (until the chip is destroyed). For example, if a suitcase is going from hand to hand, you can infer that it could be owned by a company that lends it to its employees while travelling, but it could also be a suitcase used by drugs dealers. The transaction threat also opens the way to monitor and record social networks, combined with other threats mentioned above. If some product goes from one person to another, you can infer they know each other and draw a link between them. Step by step, you can draw a complete social network, joining all the links connecting people.

Breadcrumb Threat:

The breadcrumb threat is the issue that links someone to the objects he buys; as long as the objects exist (i.e. the tag is working). When someone buys a product in a retail shop, the tag information is stored in the shop database (or even a larger database) and is not updated after the consumer's purchase. It can then create some troubles to the owner in case of a misuse by a third person. For example, let's imagine someone that buy a butcher knife, use it for a few years and then throw it away when the blade is not so sharp anymore. If another person finds the knife in garbage and uses it for a crime without leaving a fingerprint, the only reliable information will be the first buyer of the knife.

As shown, RFID systems are vulnerable to a number of attacks and hence have the potential to pose tremendous privacy and security issues for users and carriers. Nevertheless, since RFID systems are mostly used to identify objects, and since many privacy and security issues are the consequence of unauthorised reads or eavesdropping; a well-designed middleware, where object and personal data get combined, may offer a good degree of protection by keeping these two important pieces of data separated. With this, although object identity can be fraudulently read, it cannot be combined with personal data and therefore privacy is protected to a certain extent. This is the very principle of ASPIRE's privacy approach.

2.3 RFID and Privacy – position of various stakeholders

This section summarises the overall position of RFID stakeholders in regards to the security of the technology and protection of privacy. However, there are no reliable statistics or surveys reflecting this input so this version is only indicative and represents what is available on the general press, and the opinion of the writers of this deliverable. For this reason, the content of this section should not be taken "face value" or scientifically, but rather as a (hopefully unbiased) approximation of the perceived general position of RFID stakeholders.

Industry (end-users): these are rather interested in the economic benefits from

RFID, and many of them have so far overlooked concerns about its social acceptability. However, some RFID adopters such as Marks & Spencer (M&S) have adopted a responsible attitude towards RFID and therefore diverged from standards and practices that put consumers at risk. For instance, M&S RFID practice involves the manual removal of tags by employees before goods are given to shoppers. Similarly, Benetton withdrew from RFID when it realised its social implications.

The general attitude of RFID end-users in regards to the social acceptability of this technology is nevertheless changing, possibly because of the strong intervention of such other stakeholders as the European Commission, independent researchers and journalists, and NGOs European Digital Rights and BEUC – among many others. Moreover, end-users are realising that putting consumers at risk is not good for their business (!), and that RFID poses important risks of litigation by affected consumers.

Standardisation bodies and guideline-producing organisations: many of these organisations have promoted their RFID standards despite the social concerns around this technology. For instance, the dominant RFID guideline-producer, EPCglobal, has insisted on the manual disabling or "killing" of the tag at the point of sale, even though many consumer organisations and privacy advocates have pointed out the unsuitability of this solution.

European standards bodies such as ETSI and CEN seem much more oriented towards finding standards and best practices which are socially acceptable and more in line with European values. They also admit that RFID is still an immature technology in need for further research, development and standardisation; especially on privacy enhancing technologies and practices, related legislation, and social and environmental acceptability of RFID.

Governments and regulators: these have issued a number of guidelines and recommendations, specially the European Commission which has a very active approach to RFID and is strongly concerned about the social acceptability of this technology, and about finding alternatives that do not require a trade-off between economic benefit and social acceptability. The Commission must also protect the privacy and security of European citizens as required by many Treaties and Conventions, specifically by the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950. Articles of this convention relevant to these Privacy Specifications are the right to privacy (Art. 8) and the right to freedom of expression (Art. 10).

The following list contains some of the comments and recommendations to date issued by some governments and regulators:

1.- The American NIST points out[11]:

"*Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. As people possess more tagged items and networked RFID readers become ever more prevalent, organizations may have the ability to combine and correlate data across applications to infer personal identity and location and build personal profiles in ways that increase the privacy risk*" (pp ES-2).

2.- Last year, an editorial article about wireless pervasive technologies in The Economist highlighted[12]:

"*A greater concern in the long term is privacy. Today's laws often assume that privacy*

is guaranteed by a pact between consumer and company, or citizen and state. In a world where many networks interconnect on the fly and information is widely shared, that will not work. At a minimum, wireless networks should let users know when they are being monitored".

3.- Working Party on the protection of individuals with regard to the processing of personal data (European Commission)[13].

On 19th January 2005, this Working Party published a working document on data protection issues related to RFID. This working party was set up under Directive 95/46/EC to analyse the RFID technology and its implications with regard to data protection matters, study applications, privacy and security issues, guidelines and technical solutions. Specifically, to a) provide guidance to companies deploying RFID on the application of the basic principles set out in EC directives; and b) provide guidance to manufacturers of the technology as well as RFID standardization bodies on their responsibility towards designing privacy and compliant technology.

The work of this working party is critical and demonstrates the limitations and threats of the existing RFID technology, and even the unsuitability of current legislation and regulations to deal with RFID privacy and security. Section 2.6 elaborates on the findings of the working party as to the suitability of current legislation to deal with privacy and security issues associated with RFID.

4.- After holding a Public Consultation on the RFID Technology during 2006, the European Commission points out[14]:

"*4.1 RFID security and privacy*

Privacy and security should be built into the RFID information systems before their widespread deployment ("security and privacy-by-design"), rather than having to deal with it afterwards. The requirements of both the parties actively involved in setting up the RFID information system (for example business organisations, public administrations, hospitals) and the end users that are subjected to the system (citizens, consumers, patients, employees) must be considered during the design of this system. As end users typically are not involved at the technology design stage, the Commission will support the development of a set of application-specific guidelines (code of conduct, good practices) by a core group of experts representing all parties. To this end, all security related activities and initiatives will be conducted in line with the strategy for a Secure Information Society set out in COM(2006) 251.

[..]

4.3 Research and innovation policy

RFID technology is still an area of active research and development. Cost reductions of passive tags to less than 1 cent, needed for mass application, require two complementary avenues of research: further miniaturisation of silicon chips through innovations in design and assembly; research on non-silicon organic materials that hold the promise to produce printable RFID tags. More research is also needed on security (authentication, encryption) and larger rewritable memories. Future applications will need larger memories, more complex cryptographic engines, active networking capabilities, integrated sensors and power management techniques. The 2007-08 work programme of the ICT theme of the 7th Framework Programme (2007-2013) has identified four challenges which mention RFID in a number of situations (healthcare,

intelligent vehicle and mobility systems, micro and nanosystems, organic electronics, and future networks) as well as the eMobility Platform. In the future, the Commission will stimulate research on security of RFID systems, including light-weight security protocols and advanced key distribution mechanisms, with a view to preventing direct attacks on the tag, the reader and the tag-reader communication. In response to the results of the European consultation, the Commission will also support further development of privacy-enhancing technologies as one means to mitigate privacy risks".

5.- The European Commission and European Union have also issued other Communications applicable to the case of RFID and ASPIRE, being the most relevant:

- Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007) 228 final. This Communication is intended to determine the objectives to accomplish a better protection of personal data by using the so-called Privacy Enhancing Technologies.
- ARTICLE 29 Data Protection Working Party: Working document on data protection issues related to RFID technology. Document adopted by the Working Party on the protection of individuals with regard to the processing of personal data (set up under Directive 95/46/EC). It analyses RFID technology and its implications with regard to data protection matters, studying applications, privacy and security issues, guidelines and technical solutions.

6.- The Institute for Prospective Technological Studies recommends[15]: "Europe could further stimulate research on security of RFID, including the passive RFID tags which are less investigated in academic research, and including security architectures of RFID systems".

7.- Similarly, the European Commission recently held an online recommendation on RFID and privacy[16]. Whilst, at the time of this writing, the final results had not been published yet and therefore could not be included in this version of the document; these will be included as possible in and in all ASPIRE design, development and implementation activities and reflected as additions to other future deliverables. However, in its original draft the European Commission was recommending the automatic deactivation of RFID tags at the point of sale when personal data is involved. Since ASPIRE has purposely designed mechanisms to separate personal and object data and so alley some of the privacy and security issues around RFID, these recommendations fall within the spirit of ASPIRE.

To sum up, governments and regulators have been very active in the field of RFID, and have shown a very responsible mediating approach towards the improvement of this technology, predominantly of its social acceptability.

Industry (technology vendors): whilst most technology vendors have embraced RFID in a responsible way, some technology vendors have focused on the promotion of RFID in spite of its social unsuitability, and have rather focused on: (a) the need of "consumer education" as a way of shifting their corporate responsibility to consumers and citizens; (b) erroneously highlighting the effectiveness of tag "killing" or "disabling" – otherwise rejected by other RFID stakeholders; (c) stressing the otherwise unproven sufficiency of the e-Privacy Directive to deal with RFID threats; and (d) attacking or discrediting efforts by responsible stakeholders such as consumer associations or the Commission.

Most technology vendors also fear regulation or lack of global standardisation in the case of RFID, and therefore do not want privacy and security issues to rule the RFID

agenda – and therefore compromise their RFID investment and commercial possibilities.

Consumers, NGOs and other independent associations: most consumer associations, human right promoters and other NGOs have strongly opposed the current RFID proposal, particularly the item-level tagging of FMCG. Among the most active opponents we can mention the European Digital Rights, the American CASPIAN, and the European BEUC and ULD. A position statement has been issued[17]. All these and many other responsible organisations have warned about the perils of uncontrolled RFID, and pressed for the responsible use of this technology.

2.4 Possible solutions for the RFID privacy and security issues

Whilst it is not the aim of this document (and the ASPIRE project) to solve all privacy and security concerns posed by RFID, we discuss possible solutions to help the reader understand the issues and scope of the ASPIRE project in regards to the protection of consumers and industry.

As illustrated above by the figure "Conception of the challenges of RFID (and some solutions)", possible solutions for the privacy and security issues are: (a) self-regulation by industry; (b) new legislation; (c) data protection; (d) privacy and security enhancing technologies (PETs); (e) consumer self-protection – e.g. by education etc. A detailed examination of these solutions follows:

Self-regulation by industry: in this approach, industrial players (end-users, technology vendors) engage in a "moral" agreement to respect and protect privacy and security of consumers and other users. This is the easier approach because it requires no new legislation, research and development, or the standardisation of best practices. However, practice has proven the ineffectiveness of self-regulation by industry – e.g. the case of The Internet. Moreover, privacy violations are very difficult to prove due the high fluidity and liquidity of information, which can be copied and transmitted without leaving trace. For this reason, violations of the self-regulatory "code of practice" would be very difficult to prove, and companies with therefore have little incentive to act responsibly.

New legislation: in this approach, the use and applications of RFID are regulated by law. The scope of this ranges from providing sufficient information to consumers, to enforcing the use of privacy enhancing technologies, to mandating the adoption of best practices, to establishing fines or punishment for violators. Some extreme groups are even pressing for a total ban of this technology. However, the formulation of RFID-specific legislation is very difficult due to a number of reasons. Firstly, RFID is a global phenomenon and countries where regulation takes place will have economic disadvantages with respect to countries where a "laissez-faire" approach is preferred. Secondly, any legislation will definitely hinder further innovation. Thirdly, the legislation of such an immature technology as RFID is very challenging because the technology and its full impact are still not fully understood. Finally, the formulation of RFID-specific legislation would stifle and delay ongoing RFID initiatives, and make this revolution lose momentum.

Data protection: many experts are currently discussing the suitability of existing legislation and regulations for the case of RFID, particularly the e-Privacy Directive. However, we believe that the e-Privacy Directive and other related legislation and recommendations are only partially suited for the case of RFID. This is fully discussed in section 2.6.

Privacy and security enhancing technologies (PETs): these are improvements of the RFID technology that feature privacy and security by design and by default. Among these we can mention more secure RFID tags and protocols – e.g. by using encryption; the automatic destruction or disabling of tags at the point of sale; RFID tags that require passwords or are activated through mechanisms that require direct or indirect user consent – e.g. pressing a button; and algorithms that protect privacy and security at software level – the ASPIRE approach. In the field of PETs there is no "silver bullet", and different approaches are required to guarantee privacy and security issues at different levels and/or in different applications; and to various extents.

Despite the fact that there are a number of PETs in existence – either commercial or experimental, most existing RFID technologies and dominant standards and guidelines do not consider privacy and security within their technological proposal. For one, the dominant RFID guiding body, the Auto-ID Centre which subsequently gave place to the ongoing EPCglobal/GS1, seems "stuck" at self-regulation and tag disabling at the point of sale. One possible explanation for this is that this set of standards and guidelines surged from technical and functional needs (from end-users) that did not consider social issues from inception – hence the need to "patch" their developments with the "emergency" option of disabling tags. For the same reason, there is a possibility that the current RFID situation is one of over-standardisation where such dominant standards as EPCglobal are hindering further innovation and therefore the improvement of this technology, particularly on the privacy and security domains. Of course, our statement is speculative so more research in this direction is suggested.

Finally, there is an urgent need to undertake further research in PETs, not only at software level as ASPIRE is aspiring; but also at tag, reader and protocol level. In the end, only PETs have the potential to solve most if not all privacy and security issues associated with RFID.

Consumer self-protection: another option is to educate consumers so everyone knows how to protect his or herself from the perils of RIFD. Consumers could learn to find and remove or disable all RFID tags on their property or groceries, or to block these – e.g. by using "jamming" or other security devices. However, it is clear that this approach is incomplete and unreliable because some vulnerable groups will surely fail to grasp the perils and protecting measures associated with RFID. Specifically, the elderly, children, tourists and technology-unaware people may fail to understand the threats and act upon them.

For this reason, the search for a reliable privacy-friendly and secure RFID approach that works by design and by default is still ongoing, and the debate continues.

2.5 Review of The ePrivacy and other Data Protection Directives

At the moment, the most relevant legislative and regulatory approach for the RFID case is the ePrivacy Directive. However, there are other applicable Directives and legislation such as the Data Protection Directive. This section summarises the relevant legislation and its implications for the RFID process and ASPIRE. The relevant Directives are:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and of the free movement of such data (OJ L 281, 23.11.95, p. 31): applicable to both automatic and non-automatic processing of personal data, this Directive, also known as the ePrivacy Directive, establishes the main principles for a lawful

processing, and it is considered as the most important EU legal text when it comes to Data Protection.

- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 24, 30.1.1998, p. 1–8 – Derogated by Directive 2002/58): this directive particularises and complements the above Directive 95/46/EC, and aims to harmonise the provisions of the different Member States protecting the right to privacy with respect to the processing of personal data in the telecommunications sector, and to guarantee the free movement of those data across the EU.
- Directive 2002/21/EC of the European Parliament and the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive – OJ L 108, 24.4.2002, p. 33): establishes a harmonised framework for the regulation of electronic communications networks and services. It lays the foundation in the form of horizontal provisions serving the other measures: the scope and general principles, basic definitions, general provisions on the national regulatory authorities, the new concept of significant market power, and rules for granting certain indispensable resources such as radio frequencies, numbers or rights of way. This Directive is part of what is called the "Telecoms Package".
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31.7.2002, p. 37): deals with a number of issues such as (data retention), the use of cookies and the inclusion of personal data in public directories, among others. Also part of the "Telecoms Package".
- Amendment: Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006, p. 54).
- Amendment: Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communication networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) 2006/2004 on consumer protection cooperation COM(2007) 698 final 2007/0248 (COD).

The history and details on these Directives are large and complex and unnecessary for this analysis, so we do not elaborate on these. Conversely and as follows, we focus on their main concepts and substance, and on their implications for ASPIRE and the RFID process.

Definition of Personal Data and relationship with RFID

These Directives clearly define the concept of "Personal Data". Particularly, the definition of "Personal Data" is established in the Article 2(a) of the Directive 95/46:

"*'Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".

The definition of Personal Data is essential to our analysis because it determines whether RFID is covered by the Data Protection Directives or not, and determines what can be done in the context of ASPIRE as to protecting the privacy and security of citizens. In general, there is consensus that the ePrivacy and other European Data Protection Directives apply yet not suffice in the case of RFID, although this depends on the specific application. This is because the unique identification code associated with RFID-tagged objects carried by or owned by individuals can be used to indirectly identify them. Moreover, it can also be used to determine object nature (e.g. a specific medicine) and indirectly identify some of the physical, physiological, mental, economic, cultural or social identity factors of the individual. Applications where personal data and item-level tagging are involved seem to fall within the scope of the Data Protection Directives, whereas applications where RFID tags are applied to objects which are not carried or owned by individuals seem to be outside its scope – e.g. the tagging of pallets or cases.

To err on the safe side of the legislation and for the purpose of this analysis and the design, development and implementation of ASPIRE; we assume that all applications involving the item-level tagging of objects with RFID tags fall within the scope of the ePrivacy and other Data Protection Directives, and must therefore be implemented through PETs within ASPIRE's developments.

Data Controller

The concept of Data Controller establishes who collects and processes the data. The Directive 95/46 defines Data Controller as: "*the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*".

In the case of RFID, the data controller is the user of the tag. This entity determines the purpose of that tag used in combination with the network of readers and other means such as databases and information systems. One complication in the case of RFID is that third parties can access the identity and other information stored in some type of tags, particularly inexpensive passive ones – those proposed for item-level tagging. In these cases the Data Controller has limited control on the access to data, even when these data may directly or indirectly classify as Personal Data.

Consent

The applicable Treaties and Directives set limits within and beyond which the collection and process of Personal Data about an individual requires his or her unambiguous consent:

- Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 states that "*Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*".
- Art. 7 of the Directive 95/46 establishes the principles of legitimate data processing, highlighting the importance of consent: "*the data subject has unambiguously given his consent*".
- Art. 8 of the Directive 95/46 furthers the need for consent when special categories of processing apply, particularly personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life. In this sense, it also requires "*unambiguous consent*" for the collection and processing of this data.

- Art. 26 of the Directive 95/46 establishes the conditions under which data can be transferred to a third country which does not ensure an adequate level of protection, specifically the need for consent: "*the data subject has given his consent unambiguously to the proposed transfer, or [..]*".

In the case of RFID the concept of consent is more challenging because some of these devices seamlessly provide information to any compatible reader. For instance, even if the individual fully understands how the technology works, it is not clear what the acceptable extent of consent is. For example, consent to gather and process RFID data related to Personal Data may be limited to a specific shop, to just one transaction, to one day of transactions, or to an entire year of data collection. Similarly, it may be related to one or more applications. As we will see below, ASPIRE considers a definition of consent that is the most restrictive (and therefore the most protective of consumers' privacy and security rights).

Principles of the ePrivacy Directive

The principles of the ePrivacy and other Data Protection Directives most relevant to our analysis are: (1) limitation, (2) quality, and (3) conservation, as established by Art. 6 of the Directive 95/46. A summary of the principles applicable to RFID follows:

Limitation: this principle establishes that Personal Data should be processed for the intended purpose only. Further processing is prohibited. In the case of RFID, this means that any transactions generated by the RFID system (e.g. when tracking and tracking objects in a retail shop), and that could potentially be linked to the Personal Data of the carrier (e.g. the shopper) cannot be used for such other purposes as collecting individual preferences or consumer behaviour at individual level; or registering the property of individuals. It also limits the use of RFID data which could potentially identify a customer to generate unsolicited publicity or promotions.

Quality: all collected data must be relevant for the intended purpose. Data which is not relevant for the purpose should not be collected. In the case of RFID, this means that Personal Data about an individual should not be linked to object data unless strictly necessary. For example, data that identifies a consumer who pays using his or her credit card or who uses his or her loyalty card should not be linked to the identification of the RFID tags on the objects being acquired. Similarly, RFID data produced by tags on objects that have been previously acquired in the same or other shop should not be collected and/or related to other Personal Data of the individual.

Conservation: Personal Data should no be stored and/or processed longer than necessary for the intended purpose. After the purpose has finished, these data have to be deleted. In the case of RFID, this means that any RFID data which could potentially identify the individual (e.g. the identity of tags on his or her shoes), and that must be collected for lawful purposes (e.g. service, warranty or returns) should not be kept for longer than necessary for these purposes (e.g. longer than the warranty or return periods).

Other rights and principles stated by the Directives

Apart from the aforementioned concepts and principles, the ePrivacy and Data Protection Directives establish rights as to the transference of Personal Data to countries with laxer data protection legislation; give individuals the right to access, rectify and delete their Personal Data; and establish especial considerations when data include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union

membership, or health or sex life.

The design, development and implementation of ASPIRE will incorporate these and other Data Protection principles within its technology and best practices, and so protect consumers and the general public from the privacy and security threats associated with RFID. Sections 4.4 and 8 will elaborate on the implementation of the ePrivacy and other Data Protection Directives in the project ASPIRE.

2.6 Analysis: are The ePrivacy and Data Protection sufficient for RFID?

The Working Party mentioned in section 2.3 concluded that most RFID threats fall within the Data Protection Directives. However, it also recognises that "It should be noted that RFID systems are very susceptible to attacks" and recommends the destruction or disabling of the tag at the point of sale. Moreover, it recommends: "The design of RFID tags, RFID readers as well as RFID applications driven by standardisation initiatives may have a great impact in minimising the collection and use of personal data and also in preventing any unlawful forms of processing by making it technically impossible for unauthorised persons to access personal data."

In this line and concerning RFID, the aforementioned communication on Radio Frequency Identification in Europe: steps towards a policy framework, stated that a number of changes might be needed in the Privacy and Electronic Communications Directive to also embrace RFID applications, as part of the EU Telecom Rules' review. The scope of the ePrivacy Directive is not as wide as the Data Protection Directive's one: the former is limited to "the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks."

Moreover, in November 2007 a "Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and user's rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation34" was adopted. The proposal, part of a legislative package intended to amend the current framework regulating electronic communications, seeks to introduce a number of amendments in the two mentioned Directives. Concerning the ePrivacy Directive, the text establishes that "[...] the main proposals are as follows: [...] clarifying that the Directive also applies to public communication networks supporting data collection and identification devices (including Contactless devices such as Radio Frequency Identification Devices)". Therefore, this Proposal is aimed to clear up the conditions for RFID to fall within the scope of Directive 2002/58/EC.

However, whilst all current studies and publications have focused on whether RFID-related data can be directly or indirectly considered "personal data" in some circumstances and applications, and therefore whether the Data Protection Directives suffice to cope with RFID threats; most studies have failed to overtly address the perils of RFID beyond the point of sale – e.g. when personal data is not involved and/or RFID is abused by third parties. Specifically, the fact that most RFID numbering schemes (e.g. EPCglobal) reveal product characteristics (e.g. product type), and that these can violate privacy and compromise security even if no personal data is involved, has been systematically overlooked in the RFID analysis. For example, a terrorist could set a "bobby trap" to explode when an RFID-tagged copy of the "Old Testament" is detected; or a snooper can detect RFID-tagged medical implants or confidential medicines on

people passing by.

Obviously, since the ePrivacy and other Data Protection Directives were conceived to regulate the use of data between two parties "controller" and "individual", these do not cover the case when privacy- or security-related RFID data (e.g. the identity of privacy- or security-sensitive objects) can be abused by third parties. Furthermore, most RFID tags can be interrogated surreptitiously by any party so the definition of consent loses ground.

Because of this, we believe that the ePrivacy and Data Protection Directives do not suffice to legislate in the case of RFID; although suffices to cope with many of its threats, principally those addressed by the ASPIRE project. At least, our initiative to incorporate the ePrivacy and other Data Protection Directives in ASPIRE is a good start, as explained in the following section.

2.7 The ASPIRE focus on Personal Data

Although we recognise as explained in 2.6 that RFID poses privacy issues beyond the protection of Personal Data, it is not within the scope of our project (and it has never been) to solve all privacy and security issues posed by this technology. The reason is that, more than PETs, these issues require further legislation and regulation which are not within ASPIRE's possibilities. Conversely, our project will focus on the enforcement of the current Data Protection Directives, particularly the ePrivacy Directive, to improve the privacy proposal of RFID.

The ASPIRE focus on Personal Data means that our middleware will, as far as possible, keep object and personal data separated. It also means that personal data will be treated accordingly to the specifications in the ePrivacy and other Data Protection Directives. By doing so we guarantee that the identities of objects which can be used as identity proxies for people (e.g. shoes or clothing) are disassociated and do not automatically come beyond the above definition of Personal Data. Furthermore, ASPIRE will incorporate the principles of the ePrivacy and other Data Protection Directives in its logic and implementation procedures. By doing so we facilitate and guarantee the enforcement of these Directives in all ASPIRE implementations.

However, ASPIRE does not limit itself to the implementation of the Directives. It also considers other fundamentals for the protection of consumers' privacy and security:

- **Transparency**: to guarantee that the principles are fairly reflected.
- **Consumer education**: to guarantee that consumers understand the ASPIRE approach to privacy protection, can exert their right to choose, and can understand the advantages and limitations of our approach.
- **Auditing and certification**: to guarantee that the principles and practices are fairly implemented.

These fundamentals are explained more in detail in Section 4.

To conclude, the reader can think of ASPIRE as a technical implementation of the principles of the Data Protection Directives directly applicable to the case of RFID, plus other technical and operational privacy- and security-enhancing approaches.

Section 3 End user requirements – Analysing survey data

3.1 The Privacy Survey

As part of ASPIRE and to properly reflect the needs of the final users; we have conducted a Europe-wide survey where requirements related to privacy and security of consumers were collected.

Questions indirectly related to privacy and security deal with the organisation's mail product and activity. The list of products was designed to maximise functional input for the ASPIRE design, and more particularly functional input as to the privacy sensitivity of dealt products and activities. Respondents could choose from the following products:

1. Apparel or clothing (including lingerie)
2. Fashion (handbags, wallets, suitcases etc.)
3. Footwear
4. Travelling, sports or camping
5. Real (expensive) jewellery
6. Imitation (inexpensive) jewellery
7. Personal hygiene (deodorant, sanitary towels, nappies etc.)
8. Cosmetics or cosmetic implants (wigs, silicon implants etc.)
9. Corrective glasses, sunglasses, contact lenses or related accessories
10. Medicines or medical implants
11. Food or beverages (including alcoholic and other drinks)
12. Portable consumer electronics (e.g. mobile phones, music players etc.)
13. Books, newspapers or magazines
14. CDs, DVDs or similar
15. Other privacy-sensitive products – see (1)
16. Other portable products – see (2)

Similarly, respondents could choose from the following activities:

1. engineering
2. Manufacturing
3. Distribution
4. Servicing
5. Sales or rental

The main question directly related to privacy and security was: "*21. About your customers personal data. Personal data is data that, either individually or combined, can potentially identify a person or group of persons, typically: name, nickname, national ID, passport number, nationality, date of birth, credit/debit card number, bank account number, service account number, affiliation or membership numbers, car numberplate, mortgage or loan account numbers, loyalty card number, driver license id, social security number, address, fixed or mobile phone numbers, email or IP address, website, usernames to access computers or websites, biometrics (photo, fingerprint, iris pattern, voice etc.). Select the appropriate degree applicable to each question in the list below*".

Related to this question, the sub-questions in the survey were:

a. Does your business require collecting personal data about direct or indirect customers or other individuals?
b. Does your business involve buying or selling personal data about direct or indirect customers or other individuals?

c. Does your organisation have formal procedures and systems to manage personal data about direct or indirect customers or other individuals?
d. Does your business require keeping track of items bought or rented by customers for statistical, warranty, service, return or other purposes?
e. Does your business require keeping track of customers who received services for statistical, warranty, service, return or other purposes?
f. Does your country have in place legislation and mechanisms to protect personal data and enforce customer privacy?

For each question, respondents were asked to choose one from the following options:

1. Answer unknown
2. Never / no / none
3. Exceptionally / some
4. To a lesser extent / most likely
5. To a high extent / yes

Questions one and two establish whether the business involves collecting or acquiring personal data – otherwise this business is exempt from any privacy considerations by ASPIRE. The third question explores the knowledge and awareness on the need to properly manage Personal Data. This helps to value the commercial importance of protecting customer privacy. The fourth and fifth questions analyse the need to link object and personal data – which is ASPIRE's main focus regarded the protection of privacy. The final question reveals awareness on existing legislation or regulations as to protecting customer data.

Among other valuable input, the analysis of results allows knowing: (a) what percentage of businesses and what specific industries, sectors and products deal with personal data; (b) which ones would be exposed to privacy violations when they use RFID, and to what extent; (c) the extent of the necessary effort to educate end users in privacy-related regulations and practices.

In brief, this survey helps us to focus our efforts to make ASPIRE truly privacy-friendly and adapted to the European requirements.

3.2 Survey results

The survey did not reach a broader audience due to time and resource constraints. For instance, countries which organised Information Days earlier in the project calendar (as planned) obtained little response because there was not enough time to disseminate these events.

Nevertheless, the Consortium managed to receive an adequate number of responses and so obtain sufficient input to analyse privacy requirements and design these privacy specifications. Statistics on results follow:

158 organisations accessed the questionnaire, although only 51 of them provided full input and 135 provided partial valuable input. For unknown reasons many respondents skipped some of the answers, or interrupted the completion of the survey.

However, the partial and full responses are considered sufficiently representative to draw conclusions, particularly as to privacy and security issues. Moreover, at the time of the writing of this report some ASPIRE partners were holding further RFID information

days. This means that there is a strong possibility of obtaining more responses and therefore increasing the accuracy of this analysis – which needs update anyway to reflect the results of the online consultation on RFID Privacy currently under analysis by the European Commission.

The breakdown of complete answers by language is:

French:	21 valid answers
English:	6 valid answers
Greek:	24 valid answers
TOTAL:	**51 valid answers**

Apart from the questions listed in 3.1 there was other question related to the issue of privacy and security: that of the type of product. As to their main product, 46% of respondents produce food or beverages; 16% electronic products; and 12.5% medical implants or medicines. 52% of activities relate to the manufacturing of these products; and 44% relate to the servicing of these products. Secondary products follow a similar pattern.

The result of questions related to privacy and security (those listed in 3.1) are:

Sub-question	Answer unknown	Never / no / none	Exceptionally / Some	To a lesser extent / most likely	To a high extent / yes	Response count
a. Does your business require collecting personal data about direct or indirect customers or other individuals?	3	**14**	6	**11**	**7**	41
b. Does your business involve buying or selling personal data about direct or indirect customers or other individuals?	3	**34**	1	1	0	39
c. Does your organisation have formal procedures and systems to manage personal data about direct or indirect customers or other individuals?	8	**11**	8	3	9	39
d. Does your business require keeping track of items bought or rented by customers for statistical, warranty, service, return or other purposes?	5	5	7	**12**	10	39
e. Does your business require keeping track of customers who received services for statistical, warranty, service, return or other purposes?	4	4	4	11	**14**	37
f. Does your country have in place legislation and mechanisms to protect personal data and enforce customer privacy?	4	0	1	4	**27**	36

Table 3: sub-questions and answers related to privacy

In this table, we are highlighting the responses underpinning the analysis in next section.

3.3 Impact of results on privacy specifications

From the results shown in section 3.2 we can draw some important intermediate conclusions conditioning the design of ASPIRE:

1.- The products manufactured, traded or serviced by respondents require a high level of security and privacy. For example, food and beverage (46%) are subject traceability requirements to ensure quality (e.g. freshness of food) and origin (e.g. anti-counterfeiting of wine etc.). Similarly, electronic products (16%) tend to be expensive (e.g. mobile phones) or compromise privacy as they are carried around. These statistics

also suggest that security from RFID is more relevant than privacy, although the difference is not significant.

2.- There is a significant amount of Personal Data involved, as shown by question "a" where 44% of respondents require their collection.

3.- The definition of Personal Data is not clearly understood. Question 21 of the Survey defines Personal Data as follows: "*21. About your customers personal data. Personal data is data that, either individually or combined, can potentially identify a person or group of persons, typically: name, nickname, national ID, passport number, nationality, date of birth, credit/debit card number, bank account number, service account number, affiliation or membership numbers, car numberplate, mortgage or loan account numbers, loyalty card number, driver license id, social security number, address, fixed or mobile phone numbers, email or IP address, website, usernames to access computers or websites, biometrics (photo, fingerprint, iris pattern, voice etc.). Select the appropriate degree applicable to each question in the list below*". However, answers in sub-questions "d" and "e" show a clear contradiction with answers in sub-question "a": whilst only 44% of respondents indicated in this latter question that they do collect some sort of Personal Data; 56% and 68% of respondents indicated the need to keeping track of customers or sold items respectively, which necessarily requires the collection of Personal Data.

4.- Another conclusion of the results from sub-questions "d" and "e" is that many businesses are unaware of the threats related to linking Personal Data and object data – hence do not consider the latter as identifying data for customers or employees.

5.- As shown by sub-question "b", businesses rarely engage in the buying or selling of Personal Data.

6.- As show by sub-question "c", most organisations lack formal procedures to manage and protect Personal Data.

7.- As shown by sub-question "f", most organisations are aware of the European regulations on the collection and use of Personal Data.

The findings suggest that ASPIRE should focus on:

a. Clarification of the concept of Personal Data and its relationship with its link between object data in the context of RFID.
b. Breaking the link between object and personal data as originally suggested. This is because most organisations do not see this link as an extension of the identifying data associated with customers or employees.
c. Creation and enforcement of formal procedures to collect, manage and protect Personal Data.
d. Incorporation of the regulation in the software logic and procedures proposed by ASPIRE.
e. Incorporation of explanatory documents so adopters can increase their knowledge of current privacy and security regulations.

Conversely, the findings suggest that ASPIRE should not invest significant efforts on inter-organisational transmission of object and personal data because most respondents do not trade with these.

Section 4 Fundamentals of ASPIRE's privacy specifications

4.1 Transparency and open source software

The Commission and other RFID stakeholders have recommended increasing the transparency of information systems, above all those dealing with personal data and other sensitive data such as financial or health data.

However, increasing the transparency of information system is not easy, more than ever under the current economic paradigm that favours intellectual property and industrial secrets. Most RFID software to date is based on proprietary technology because of intellectual property issues: vendors want to avoid competitors and free-riders to copy and use their products, as it would be the case with OSS. Whilst lack of transparency is convenient for business because it allows companies to protect their development and hence their investment, the same lack of transparency means that consumers, governments, citizens and other companies are forced to trust suppliers to not to intentionally or accidentally compromise the security (and hence the privacy) of data in these systems. For example, whilst most people on the world use MS Windows as the operating system for their personal computers, this system is closed and opaque and we must trust Microsoft not to spy on our data, and to provide a system secure and reliable enough not to allow third parties to spy on our data. This is particularly and increasingly important as most computers are nowadays connected online, and more and more personal and confidential data is entered into them.

In a nutshell, increasing the transparency of information systems is desirable from a social point of view, but undesirable from a business point of view.

ASPIRE's approach to transparency means that our source code will be distributed under an OSS license. This gives all RFID stakeholders the possibility to directly (e.g. by direct observation) or indirectly (e.g. through specialised trusted partners) examine the code and so determine whether their data is properly and legally looked after. It also gives the possibility for contributors other than the original developers and owners to detect and fix security or privacy flaws, and improve the functionality of the system.

More specifically, the transparency of ASPIRE will allow stakeholders to:

- Show the privacy and security methods implemented by ASPIRE.
- Allow the detection and correction of security and privacy flaws by an audience broader than with proprietary developments.
- Improve the security, efficiency and functionality of the system.
- Allow the public auditing of privacy algorithms and practices.
- Implement certification programmes for adopters and technology improvers.

In this sense, ASPIRE is pioneer because no organisation or consortium has before proposed the use of OSS as a way of allaying privacy and security concerns through extended transparency. This idea was pioneered by the Charity Open Source Innovation Ltd and by its founder Humberto Morán, main author of this deliverable; and is being tested in ASPIRE for the first time. ASPIRE is not only an innovative approach to privacy and security: it is also a research experiment to test the limits and applicability of OSS to a completely new and promising territory: that of social acceptability of ICT.

On the other hand, the fact that ASPIRE will be available to everyone means that the Consortium partners must implement business models other than the plain licensing of

the software. These business models range from the selling of complementary products and services, to the establishment of a privacy certification programme as described below. Of course, the sustainability of these business models requires significant initial investment, mostly to create the OS solution in the first place. For this reason, the funding of the European Commission through the ASPIRE project was essential to cover the original (and challenging) costs associated with the development of hard-to-profit-from OSS.

Section 5 furthers on the importance and approach to transparency in ASPIRE.

4.2 Consumer education

Most surveys on RFID show an important lack of consumer knowledge on RFID. This is because most publications and events have focused on the same group of specialised stakeholders. A particularly relevant survey and analysis is that conducted by Dr. Sarah Spiekermann[18]. This survey of 642 participants shows little awareness on RFID privacy, yet strong concern among 15% of participants. It also shows that those people with knowledge of RFID are concerned about the lack of control and the link with personal data. Importantly, this and other studies show that people who do not fully understand RFID tend to show more opposition to this technology.

Since ASPIRE is designed to address privacy by design and by default, consumers must be informed of the privacy and security advantages of our developments, and of existing limitations. Moreover, they should be informed about the auditing and certification programmes explained below so they are given the right to choose different suppliers according to their privacy classification.

Specifically, consumer education should focus on the following topics:

- The RFID technology and its different components and alternatives,
- advantages of using RFID, not only for businesses but also for society and the Environment,
- the different privacy and security threats posed by RFID,
- their fundamental privacy and security rights,
- how to protect from the privacy and security threats posed by RFID,
- the ASPIRE approach to privacy, including the auditing and certification programmes,
- the ASPIRE privacy levels and seals, and their meaning.

In brief, consumers should be able to understand that RFID poses certain threats which are addressed by ASPIRE, and that organisations using ASPIRE and its certification programme are different from (and better than) organisations using other technologies.

This consumer education should take place with clear and simple messages, without engaging consumers in a complex and confusing technical jargon. For this purpose, the certification programme proposed in ASPIRE and explained below aims to use a simple approach to qualifying and communicating the level of privacy associated with an organisation.

Section 6 furthers on the importance and approach to consumer education.

4.3 Auditing and certification

A privacy-friendly design and consumer education do not suffice to guarantee RFID privacy. This is because the implementation of ASPIRE may be intentionally or accidentally tampered with, or the adopter may fail to implement the required procedures and practices. For example, since ASPIRE is distributed with the source code, some unscrupulous companies may be tempted to modify it to override the privacy controls. Similarly, whilst the executable or binary files may be implemented unaltered, some procedures such as backups or data transmission may not be executed in a privacy-friendly and secure way.

For this reason, ASPIRE envisages the development and implementation of an auditing and certification programme that guarantees proper implementation and use of its middleware. The purpose of this programme is two-fold:

1. Audit every implementation to verify technical and procedural compliance of ASPIRE's original privacy-friendly code and operational procedures. This involves the verification of executables and environmental software – e.g. operating system; the overall configuration of the system; and the implementation of procedures and practices. The auditing side of the programme is oriented towards industrial adopters of ASPIRE.

2. Create and disseminate certification seals to allow consumers to understand and choose the privacy level of the different ASPIRE implementations. This involves all activities requiring consumer education detailed in 4.2. The certification side of the programme is oriented towards industrial adopters, consumers and the general public.

ASPIRE does not intend to fully implement the certification programme, but to develop it and start its implementation in a couple of pilot projects. The post-ASPIRE implementation of the auditing and certification programme will be led and carried out by the charity Open Source Innovation Ltd; and co-led by the permanent ASPIRE consortium established after project completion.

Section 7 furthers on the auditing and certification programme for ASPIRE.

4.4 Incorporating the ePrivacy Directive

The last of ASPIRE's fundamentals for privacy is the incorporation of the principles of the ePrivacy and other Data Protection Directives in the design, development and implementation of ASPIRE. This involves translating the principles in the Directives into technical implementations, procedural and other implementations. Specifically:

Technical mechanisms: the principles of limitation, data quality and conservation will be translated into specific technical approaches. For instance, the principle of limitation means that personal data and its associated object data will be only used in the necessary modules and algorithms, and cannot be accessed by any other functionality in the middleware or beyond. The principle of data quality means that the RFID network and ASPIRE will not collect or store information which is not required – e.g. the ID of RFID tags which are not involved in the current transaction. The principle of conservation means that there will be background processes in charge of deleting personal data which is not longer necessary. Finally, the other principles such as access to personal data by the individual or reflecting consent to further transactions will be implemented in ASPIRE through extra-functionality and additional modules.

Procedural mechanisms: certain procedures related to the use of ASPIRE and its RFID network must also reflect the principles of the ePrivacy and other Data Protection Directives. These procedures range from the proper identification of the individual, to the proper explanation of privacy and other threats to ensure informed consent, to the proper management of backups to guarantee the conservation principle, to organisational changes and methods to ensure compliance with the privacy specifications.

Section 8 furthers on the incorporation of the ePrivacy and other Data Protection Directives into ASPIRE.

Section 5 The importance of transparency

5.1 Some privacy threats happen at software level

Privacy and security are contextual by nature. Both depend on who can access which information about whom. We do not mind sharing personal information with our friends or relatives, and even with some trusted business partners; but when it comes to sharing it with strangers the issue is completely different. For this reason, contextual factors are paramount when it comes to protecting privacy and security. These factors can only be considered in the logic of the information systems where they are combined, namely the middleware. For example, when a buying transaction takes place using a personal credit card and objects tagged with RFID chips, the individual must identify itself to prove that he is the owner of the card. If the product is subject to warranty or a service agreement, it may be necessary to link the identity on the tag to the identity of the buyer. Conversely, if the object does not need to return to the retail shop this link is unnecessary.

The context of the transaction is usually known at software level, specifically at middleware level. It is at this level where object and business information combine and may therefore give place to privacy threats. For example, if the timestamp or transaction ID is stored in both the RFID transaction and the payment transaction that involves personal data, the resulting data may compromise privacy because the object identity may be linked to the personal identity of the individual through this timestamp or transaction ID.

Software can be written in such a way that contextual factors are taken into consideration for the protection of privacy and security by eliminating, blurring or not collecting unnecessary information in the first place. Section 8 and more specifically 8.3 elaborate on these mechanisms.

This is possible, but not without challenges. Firstly, the logic in the privacy approach may be flawed or subject to bugs. Secondly, the software logic must be open to scrutiny to guarantee that it does what it intends to do. The best way of addressing these challenges is by using open source software because this allows more "minds" to cooperate in the creation of secure privacy-friendly algorithms; and exposes the privacy approach to public scrutiny and therefore ensures consumers that the system is not "spying" on them, and that the information cannot be misused.

It must be clarified that the openness of OSS applies to the source code and logic, and not to the data itself. Conversely, the data must be protected by using strong OS encryption algorithms for the storage and transmission of data.

The exposure of the system to scrutiny by the general public is based on the idea of "reciprocal transparency" suggested by the author David Brin[19]. Although this author pushes the idea to the extreme by demanding that leaders disclose their personal data (idea with which we do not personally agree); the same principle can be applied to the case of disruptive technologies. Whilst citizens are becoming more and more transparent because of the surge of sophisticated information systems and disruptive technologies, these information systems and technologies are nevertheless opaque and secretive, mostly because of intellectual property concerns. The application of "reciprocal transparency" in a more reasonable way suggests that information systems should become more transparent to ensure citizens that the data they provide is not abused or misused. In other words, to ensure proper enforcement of the applicable legislation, in

this case the Data Protection Directives.

This combination of privacy-friendly algorithms (PETs) and transparency allows creating a society where intrusive technologies are possible, but also where strong institutions can "watch the watchmen".

5.2 The opportunity of Open Source Software

As discussed before, OSS offers a unique opportunity to offer transparency and so ensure and allay consumer privacy.

Furthermore, OSS offers many other opportunities specific to RFID, as follows:

Inclusion: since ASPIRE OSS middleware will be royalty-free it will be available to all SMEs and other companies keen on reducing the total cost of ownership of their RFID systems. This will contribute to the inclusion of small supply chain partners, and therefore to the widespread adoption of ASPIRE and RFID. Conversely, the state of the art in RFID is that existing middleware solutions are expensive and therefore beyond the reach of most SMEs. This poses a problem for the adoption of RFID because about 80% of the supply chain is made of SMEs.

Standardisation: the widespread adoption of ASPIRE will also contribute to the 'de facto' standardisation of its interfaces and other standards included and considered in ASPIRE such as business practices etc. The potential of OSS to set market standards has been demonstrated by Linux, Apache (which powers two thirds of Internet servers), and Firefox; to mention some examples. We expect ASPIRE to follow a similar route and become the "Linux" of RFID.

Flexibility: the flexibility of OSS, which can be improved, extended and adapted to many requirements, will also allow the widespread adoption and continual improvement of ASPIRE. In particular, the adoption of an OSS licence that requires contributors to "feed" modifications back to the original owner guarantees that extensions and improvements will be soon made available to all stakeholders.

Collaborative approach: finally, OSS can enable such developments to be collaborative as ASPIRE where many heterogeneous partners collaborate in the creation of the middleware and associated developments. For instance, the ASPIRE project is already using collaborative software development tools that enable not only the Consortium partners to collaborate in the developments, but also other external contributors potentially interested in adopting the ASPIRE middleware or developing businesses based on it.

As explained, the choice of OSS for ASPIRE gives place to of numerous advantages, and we "aspire" to make the most of this opportunity.

Section 6 Achieving consumer education

6.1 The novelty of privacy threats

Privacy as a right is rapidly eroding in modern society. The right to privacy has so far taken for granted because it has never been threatened at such level before. The reason why privacy is eroding so quickly is the combination of a number of technological advances achieved during the last few years:

Miniaturisation: wireless devices are becoming smaller and so harder to see and locate. They are also easier to incorporate in common objects and products. For instance, some passive RFID tags such as the µ-tag are the size of a grain of sand and can be easily hidden in products. Similarly, microphones and cameras have significantly reduced their size and can nowadays be mounted in miniature robots the size of a fly.

Interconnection: wireless devices have expanded their network capabilities. These can be connected to The Internet and so achieve an unprecedented dissemination reach and speed. Whereas in the past it took months or years for news to reach distant destinations, nowadays any worthy piece of information travels around the world virtually at the speed of light. Undesired digital footprints are hard to remove because information is fluid and can be easily reproduced and stored once expressed in digital format. Importantly, the interconnection of devices also allows putting together many meaningless pieces of data into valuable information – e.g. by using databases and data mining techniques. For example, whilst the footprint of a single RFID transaction may be relatively meaningless and harmless; the "whole picture" of RFID transactions generated by objects belonging to the same person may give a precise idea of the person's whereabouts and habits.

Intelligence and automation: wireless devices are becoming more and more sophisticated. For example, mobile phones are now small computers with tremendous processing capabilities compared to those computers of only twenty years ago. Intelligence and automation mean that the data received by these devices can be processed and converted into valuable information. Although not currently applicable to most RFID tags (because of their low processing capabilities to date), other wireless devices can incorporate automatic identification technologies such as biometrics. The increased intelligence and automation of wireless devices mean that they are able to interpret the surrounding world, and hence generate more and more accurate information about us and increase privacy threats.

Low cost: according to Moore's law, the cost of computers is constantly reducing whilst performance is constantly increasing. This also applies to wireless devices. Consequently, the business viability of applications involving wireless devices is progressing and so is their ubiquity and pervasiveness. More pervasive devices mean more devices to generate an electronic footprint, and therefore more privacy and security threats.

Flexibility: intelligent wireless devices such as RFID tags are also more and more flexible in their use and applications. For instance, the powering of tags through induction has rendered batteries unnecessary. Similarly, many devices incorporate memory, location and sensing capabilities. This means that they can potentially sense and/or store personal data such as location or identification details. The flexibility of ubiquitous devices also means that these can be used in countless applications, from intelligent houses, to automated manufacturing, to object tracking, to environmental sensing. This

increases their pervasiveness and therefore the electronic footprint they leave behind.

Reliance on technology: because of its advantages, we increasingly rely on technology to perform our business or personal transactions. A good example is b2b or b2c e-commerce, or using the online Yellow pages or search engines. This has significantly increased our electronic footprint and is creating novel privacy threats for citizens. Importantly, whilst with The Internet going online and providing personal data is still voluntary (we can live without), the use of RFID tags in everyday objects such as FMCG mean that many consumers may unsuspectingly receive these wireless devices and create privacy or security threats for themselves.

6.2 Why should consumers be educated?

For all reasons explained in 6.1, citizens are not prepared for the privacy and security threats from technology, and especially from RFID. Moreover, they may not distinguish PETs from intrusive technologies and may not be able to protect themselves or exert their right to privacy. This may create unnecessary and irrational opposition to this promising technology, or (even more dangerous) allow some privacy-unfriendly technologies to establish as the industry standard. Therefore, education of consumers and the general public is an essential part of ASPIRE.

ASPIRE will emphasise its privacy and security approach, which puts consumers first to both achieve proper protection and also to extend benefits to consumers – e.g. by promoting better or fresher products.

These educational activities should pivot on simple and clear messages, emphasising differentiation from other RFID middleware so people can understand why ASPIRE's approach to RFID is far more socially acceptable than others. The education of consumers is part of ASPIRE's dissemination workpackage. However, it is the intention of the Consortium that it will continue after the conclusion of the project.

Section 7 Auditing and certification

7.1 Auditing privacy-friendly software and best practices

As mentioned in 4.3, the auditing of implementation and best practices will ensure the correct implementation of the ASPIRE middleware and its operational practices. This auditing involves the following activities:

On-site technical auditing of the implementation of ASPIRE: this involves periodic surprise or planned visits to the facilities in order to study the technical implementation, specifically the configuration of the equipment, environmental and application software, RFID network and configuration of the ASPIRE middleware. On-site visits are necessary to ensure that unscrupulous organisations do not tamper with the online auditing of the system detailed next.

Online technical auditing of the implementation of ASPIRE: to reduce auditing costs and reach many organisations, most of the technical auditing will be performed online, either manually or automatically. For this, ASPIRE adopters should open their RFID-supporting systems to the auditing organisation and allow 24/7/365 connections. Any change in the security of the system must be communicated in advance so the auditing background processes can keep with their work.

Auditing of operational procedures related to the implementation of ASPIRE: the operational procedures related to the implementation of ASPIRE will be audited to verify compliance. This will be performed through on-site visits to end users. Whilst most of these visits will be planned (e.g. annual or bi-annual); some will be surreptitious or surprise visits, more so if the end user has a story of privacy violations or when online audits have revealed recklessness or flaws.

Specialised auditing of technical or procedural modifications made to tailor ASPIRE to specific business needs: since some customers will tailor ASPIRE to their specific needs, a special certification programme will be developed to verify that these modifications have not negatively impacted in the ASPIRE privacy design. Specialised audits are expected to be rare and limited to those business that cannot accommodate their privacy and security practices within the limits of ASPIRE.

The cost of auditing will be covered by ASPIRE adopters, who will benefit from the use of certification seals to ensure their customers that their privacy and security is looked after. This certification seals are described in the following section.

7.2 Creating certification seals

To provide adopters with commercial benefits from the use of ASPIRE and the contracting of its auditing programme, ASPIRE will also create, register and disseminate privacy seals to rate the privacy and security level of each adopter and so allow it to communicate this advantage to its customers. For example, supermarkets implementing and compliant with ASPIRE will be able to show a purposely designed privacy seal either on their website, products or retail outlets. To adapt to the many possible levels of privacy, this seal will follow an approach similar to that of hotel stars, together with the ASPIRE trade-marked privacy seal (to be developed during the project).

The following table shows a preliminary approach to the tiered classification. This is

however subject to change during the project execution as it depends on new findings and developments:

0 (no stars)	No privacy considerations – consumers beware!
* (one star)	Minimum privacy considerations. Personal data is registered, linked to object data and kept for more than one year. This data might be also sold to third parties for marketing or promotional purposes.
** (two stars)	Little privacy considerations. Personal data is registered, linked to object data and kept for more than one year. This data will not be sold or transferred to other parties.
*** (three stars)	Moderate privacy considerations. Personal data is registered and linked to object data, but kept for no longer than one month. This data will not be sold or transferred to other parties.
**** (four stars)	High privacy considerations. Personal data is registered but not linked to object data or kept for longer than one month. This data will not be sold or transferred to other parties.
***** (five stars)	Full privacy. Personal data is never collected or traded.

Table 4: tiered classification of privacy

Upon the conclusion of the project ASPIRE, partners and principally Open Source Innovation will promote the use of these seals and their classification so as to provide consumers with a clear idea of what their privacy rights are when shopping.

The number of stars per organisation and facility depends on their configuration and implementation of ASPIRE. This will be determined during the auditing process, and the stars can be given or taken as audits are more or less successful respectively, or organisation can be fined if they are found in severe breach of their privacy controls and procedures.

Section 8 Incorporating the ePrivacy and other Data Protection Directives into ASPIRE

8.1 Privacy-friendly algorithms and techniques

Privacy-friendly algorithms and techniques are those designed to protect personal and other sensitive data. These intend to reduce or limit the amount or life of sensitive data in quantitative and/or qualitative terms. These also intend to protect, restrict or difficult access to sensitive data. The most important privacy-friendly algorithms and techniques to be considered in ASPIRE are:

Anonymity: this consists of eliminating the pieces of data that identify an individual, so its sensitive data becomes anonymous. Examples of data identifying an individual are his or her social security or identity number, address, phone numbers etc.

Use of pseudonymous or fake data: similar to the above, but replacing identifying data for other random or fake data. To even improve the privacy protection i.e. tracking, a list of rotating pseudonyms can be added.

Blurring: applicable to logical links between transactions such as transaction IDs, timestamps etc. This involves slightly changing this data so the previous relationship is difficult to establish. For example, it may involve randomising timestamps by ±20% to break the original relationship between object transaction and payment transaction.

Separation: this involves the physical separation of pieces of data – e.g. in different file-systems or databases; in order to make difficult the establishment of their relationships. For example, personal data may be kept in a database different than that hosting object and other company data.

Reduction of granularity: this consists of trimming data to reduce the level of detail. For example, the identity of an item-level tag may be trimmed so the item part of the code is removed so the data is only registered at the level of product type. This is more or less how retail shops work nowadays because they do not have a way to identify product at item-level.

Encryption: this involves the use of cryptography, either through private or public keys or other mechanisms. Encryption is well known in ICT and is commonly used for the safe storage and transmission of sensitive data.

Cumulative statistics: this is a simple but very effective mathematical trick to calculate statistics without registering data about individual transactions. For example, to calculate the average price of products sold in a day it suffices to add the total T and count the individual items I. The average will be given by T/I without requiring the storage of all individual transactions. Similar algorithms can be applied to find maximums and minimums, calculate standard deviation and compute other statistical data.

Shuffling: in some occasions transactions of different nature are registered in the same order. This allows putting them together as the logical relationship is still given by the order of registers. For example, even if we blur the relationship between object and personal data, if both transactions are registered in the same order it is still possible to put them together – hence breaching privacy. To avoid this we can use algorithms to shuffle either or both transaction sets.

Cleanup + overwrite: to get rid of old data we recommend cleanup background processes. These will run periodically or upon certain conditions such as arrival of new transactions or triggering of privacy alarms (see below). Moreover, cleanup processes will not just delete data using operating system or API functions: it will overwrite the previous data with dummy data to guarantee proper deletion.

"In memory" processing: this consists of processing as much of the transaction in memory as possible, and writing only the final results. For example, a payment transaction requiring object data such as price and stock levels will perform all necessary calculations in memory within the same transaction, and write the payment only (e.g. without the object data).

Copy + destroy: this involves the transfer of data without leaving a previous copy. For example, backups on data not longer necessary for daily purposes will remove these from the database once the backup is successfully completed and verified. Similarly, successful transactions sent to business partners will remove the original data if this is not longer necessary from a business perspective.

Volatile encryption: this involves encrypting data with a key that will be discarded after a period of time. For example, this can be used to backup personal data meant to be deleted after a certain period of time or under certain conditions. When this time expires or the conditions are met, the system will automatically delete the encryption key, so rendering the data irrecoverable.

Vigilance of personal or sensitive data: every process programmed in ASPIRE will require special electronic "permission" to access personal or sensitive data. This "permission" will be configured, documented and audited when the process is incorporated, and will be automatically marked to require further auditing when it changes. Any other process intending to access this data will trigger a Privacy Alarm as described below.

Filtering of non-related data: ASPIRE will automatically filter out any data which is not related to a valid transaction in the system. For example, the detection of tags which do not belong to the organisation will be ignored.

We will see in section 8.3 how these algorithms and techniques allow the incorporation of the ePrivacy and other Data Protection Directives in ASPIRE.

8.2 Privacy-friendly practices

ASPIRE will incorporate functionality and logic to support other privacy friendly practices as detailed:

Customer identification: ASPIRE will incorporate mechanisms to identify and allow individuals to connect online. These mechanisms will be similar to but simplified versions of those used by modern online banking systems, where customer authentication is essential to provide financial data. For this, ASPIRE will incorporate the concepts of customer id and password, and authenticate customers by their username and some randomly selected digits of its password. Failed identification will generate a Privacy Alarm for investigation (see below).

Access and correction of data: linked to the previous point, ASPIRE will provide interfaces so end-users can access and correct or delete their personal data according to the Data Protection Directives.

Support for automatic tag deactivation or privacy mode when available: since there is ongoing research to allow the automatic deactivation of tags at the point of sale and so protect consumers' privacy and security; ASPIRE will incorporate and enforce this functionality when possible.

Numbering of reports and backups: a common source of data leaks are paper reports or backups. These can be printed out and easily taken out of the office, so compromising privacy. The individual numbering of reports and backups allows keeping track of them and hence auditing their correct destruction or storage. For example, all reports which are not longer necessary can be sent to a single person or department in charge of destroying them and informing ASPIRE of this destruction. If any reports or backups have not been reported as destroyed or archived within the normal period of time, the system will generate a **Privacy Alarm** (see below).

Privacy alarms: these will be triggered when the above algorithms are considered ineffective due to the amount of data or operational characteristics. For example, a Cumulative Statistic with only one record (or with less than a number of records) does not "dilutes" data sufficiently to protect privacy. Similar examples apply to **Blurring, Reduction of Granularity, Shuffling** etc. Another example is the accidental or intentional interruption of the Copy + Destroy, which may leave two copies of the data where it was initially intended to leave only one. These Privacy Alarms will be sent to the system administrator, privacy manager of the organisation, or auditor of the system for examination and correction if possible.

Privacy manager: ASPIRE will also propose minor organisational changes, in particular the creation of the Privacy Manager who will be responsible for enforcing policies and practices protecting privacy, specifically:

- dealing with the top management of the company, internal and external auditors and with legal department in matters related to the protection of consumers' privacy and security,
- adapt ASPIRE's privacy and security practices to the specific needs and practices of the organisation,
- advising staff as to privacy-enhancing practices, and
- managing privacy alarms.

8.3 Implementing the ePrivacy and other Data Protection Directives at software level

The privacy-friendly algorithms, techniques and practices described above allow the incorporation of the principles in the ePrivacy and other Data Protection Directives. This section explains how these techniques will support this incorporation and make ASPIRE privacy-friendly by design and by default.

Limitation (not processing the collected information for unintended purposes): the intelligence and programmability of ASPIRE, together with the privacy alarms detailed before, will allow limiting the use of personal data for the intended purposes. This is achieved by controlling access of fixed and programmable logic to the database structures where personal data is stored (**Encryption** and **Vigilance of Personal Data**). Any new logic must comply with specific business requirements and therefore be properly configured and documented in the system so as to be properly audited by the certification programme. If any programmable logic is changed to access personal data for unauthorised transactions a "privacy alert" will be triggered and the ASPIRE

administrator and external auditor will be immediately notified.

Quality (not collecting information that is not essential): ASPIRE algorithms will address data quality by (a) limiting the amount of collected personal data to what is necessary as defined in the configuration of the system; and (b) managing the link between personal and object data so the latter cannot be misused to illicitly identify a person (does not become personal data). Data Quality will be enforced by using:

- **Anonymity, Pseudonymous or fake data**: when identification of the individual is not necessary after the transaction.
- **Blurring, Separation or Shuffling**: when personal and object data do not need to be related after the transaction.
- **Reduction of Granularity and Cumulative Statistics**: when item-level data is not essential after the transaction.
- **Filtering of non-related data**: when consumers are expected to wear tags from previous buys.

Conservation (not retaining personal data for longer than necessary): ASPIRE will incorporate "on-the-fly" transactions where the necessary data are kept only for the duration of the transaction and either deleted or "blurred" afterwards. Aspire will also incorporate automatic "cleaning" mechanisms to delete any personal data not longer necessary; and/or trigger privacy alarms requesting its deletion. Conservation will be enforced by: **"In memory" processing, Copy + Destroy, Volatile Encryption, and Numbering of Reports and Backups** when the data is not longer necessary for the normal operation of the system.

Other principles: ASPIRE will incorporate other mechanisms allowing individuals to identify themselves and access and correct or delete their personal data as required by the Directives. It will also incorporate measures for the protection of personal and object data such as encrypted storage and transmission. These other mechanisms and measures are:

- **Customer Identification and Access and Correction of Data**: to allow consumers verify, correct or delete their personal data.
- **Support for tag deactivation**: when the tag leaves the organisation.

8.4 Implementing the ePrivacy and other Data Protection Directives at business level

The operational approaches in 8.2 will be supported by a number of operational and business practices. These range from how to inform and deal with customers when personal data is provided, to the management of backups and printed reports containing personal data, to how to deal with privacy alerts, to creating the figure of the privacy manager, to how to remove or deactivate tags at the point of sale.

To implement this, ASPIRE's auditing and certification programme will incorporate recommendations for the education of staff dealing with personal and object data, and for the creation of the necessary organisational structures and responsibilities (e.g. the privacy manager).

A detailed list of recommended privacy-friendly best practices to be delivered with ASPIRE is:

- when collecting Personal Data, inform consumers of their rights (e.g. to access,

modify and delete it at any time), and procedures to exert them,
- when collecting Personal Data, limit to that strictly necessary for the business without gathering further information "just in case",
- when collecting Personal Data, make sure that the customer is properly identified,
- provide clear information as to where RFID is used and how,
- clearly mark products labelled with RFID tags,
- provide a post-POS reader so consumers can verify whether all tags have been removed or deactivated,
- print out only the strictly necessary reports,
- make sure that external auditors or support personnel (e.g. IT consultants) do not take any personal or sensitive data with them when they leave,
- establish a clear, secure and systematic backup policy ensuring that no backups can be lost unless they are properly encrypted,
- establish an encryption policy for laptops when they contain personal or sensitive data,
- establish an email checking policy to guarantee that customer or object data is not sent without using anonymity, pseudonyms or other privacy-friendly algorithms,
- remove CD/DVD writers and USB or other ports from desktops with access to the database where personal data is stored,
- for the managing of ASPIRE and enterprise systems dealing with personal or sensitive data, create an intranet separated from The Internet,
- make sure that your staff is properly trained and aware of privacy-friendly and security regulations and best practices.

Conclusions

This document has described all necessary technical and operational specifications to make of ASPIRE a truly privacy-friendly and secure RFID middleware, and hence provide consumers and citizens with a certain degree of protection.

In this sense, ASPIRE is an experiment to create a PET in an area where privacy and security are "hot topics": that of "The Internet of Things". The success of this experiment means that other software in "The Internet of Things" and even in The Internet may be able to benefit from the measures described here to improve the privacy and security of consumers and citizens, without significantly impacting on the use and adoption of beneficial technologies such as RFID.

However, we would like to be cautious and address the limitations of the privacy specifications of ASPIRE, specifically:

1. The specifications are ambitious and the first version of the ASPIRE middleware may not be able to incorporate all these. However, the publication of ASPIRE and this guiding document under OSS licenses will hopefully allow the OS Community to improve the middleware by incorporating all the privacy and security measures described here, plus others we failed to conceive. It is the purpose of ASPIRE to start the "virtuous circle" of protecting privacy and security by appealing to the collaboration and social responsibility of the OS Community and other post-ASPIRE collaborators.

2. It was noted and it must be emphasised that ASPIRE does not solve all privacy and security issues around RFID. For instance, if tags fail to be removed or disabled at the point of sale consumers may be put at risk even if tag identity has been separated from personal data as explained here. This is because some object data such as product type are also source of privacy concerns (embarrassing, personal or confidential objects), and security concerns (expensive or terrorism-sensitive objects).

On the bright side, if successfully implemented ASPIRE will solve important privacy and security issues, especially those that take place before the point of sale. For instance, the privacy and security mechanisms in ASPIRE will significantly reduce the amount of collected, processed and stored personal and sensitive data, will separate these from object data, and will provide better technical and operational mechanisms to protect these. This advantage will be also verified by an auditing and certification programme, and disseminate to consumers who then will be able to choose to buy from those organisations where their personal data are better looked after.

As we can see, all privacy and security fundamentals of ASPIRE fit together very well and ensure a high level of protection for consumers, industry and citizens; without compromising the flexibility of businesses.

We would like to finalise this document by recommending further research on those privacy and security issues not addressed by ASPIRE, particularly the creation of more secure tags that cannot be read without authorisation even if they fail to be deactivated or removed at the point of sale. The creation of these devices would "close the loop" and allow the full secure and socially acceptable deployment of RFID, with all its economic, social and environmental benefits. The ASPIRE Consortium also believes that there is a

strong need for a common RFID policy in Europe covering from standardisation, to consumer education, to social and environmental acceptability, to legislation and regulation, to research, innovation and development.

List of Figures

List of Tables

Section 9 References and bibliography

[1]"The Internet of Things", United Nations, International Telecommunications Union, November 2005. http://www.itu.int/osg/spu/publications/internetofthings/

[2] www.rfidconsultation.eu

[3] Radio Silence, The Economist, June 9th 2007

[4] Source: internal research Open Source Innovation Ltd

[5] As defined in http://www.opensource.org

[6] Source: internal research Open Source Innovation Ltd

[7] IdTechEX 2005, http://www.soc-eusai2005.net/documents/presentations/pres_84.pdf

[8] http://www.idtechex.com/products/en/articles/00000728.asp

[9] http://news.zdnet.co.uk/emergingtech/0,1000000183,39155851,00.htm

[10] Garfinkel, S.L.; Juels, A.; Pappu, R., "RFID privacy: An overview of problems and proposed solutions", Security & Privacy, IEEE.

[11] "Guidelines for Securing Radio Frequency Identification (RFID) Systems", US National Institute of Standards and Technology (NIST), Special Publication 800-98 – April 2007.

[12] The Economist, April 28th 2007, pp 12.

[13] http://www.olis.oecd.org/olis/2007doc.nsf/LinkTo/NT00005A7A/$FILE/JT03238682.PDF

[14] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGION – Radio Frequency Identification (RFID) in Europe: steps towards a policy framework", March 2007, pp 9 & 10.

[15] "RFID Technologies: Emerging Issues, Challenges and Policy Options", Institute for Prospective Technological Studies, EC JRC, EUR 22770, 2007.

[16] http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=RFIDRec

[17] http://www.privacyrights.org/ar/RFIDposition.htm

[18] "Between Extreme Rejection and Cautious Acceptance", Humboldt-Universität zu Berlin, Feb 2008.

[19] "The Transparent Society", David Brin, Perseus Books, 1998.