Ministry of Transport
and Communications

RFID in Finland

A survey of RFID deployments and privacy impact assessment (PIA)

Publications 5/2012

Ministry of Transport and Communications

Vision

Well-being and competitiveness through high-quality transport and communications networks

Mission

The Finnish Ministry of Transport and Communications seeks to promote the well-being of our people and the competitiveness of our businesses. Our mission is to ensure that people have access to well-functioning, safe and reasonably priced transport and communications networks.

Values

Courage, equity, cooperation

Ministry of Transport
and Communications

Date
28 February 2012

Title of publication
RFID in Finland: A survey of RFID deployments and privacy impact assessment (PIA)

Author(s)
Karri Rantasila, Antti Permala

Commissioned by, date
Ministry of Transport and Communications

Publication series and number
Publications of the Ministry of Transport and Communications 5/2012

ISSN (online) 1795-4045
ISBN (online) 978-952-243-289-6
URN http://urn.fi/URN:ISBN:978-952-243-289-6
Reference number

Keywords
RFID, privacy impact assessment framework, PIA, data protection, data security, NFC

Contact person
Kirsi Miettinen

Language of the report
English

Other information

Abstract

This report provides a comprehensive outlook on RFID (Radio Frequency Identification) business in Finland, covering the profile of RFID sector, legislation related aspects, implementation of Privacy Impact Assessment (PIA) framework, and user requirements concerning usability.

Due to the ability of RFID technology to operate without direct visual contact at long distances (even 6-8 meters), there is a need to privacy and data protection related legislation and recommendations in the field of RFID deployments. Furthermore, RFID infrastructure is not always easily detected by the human eye, stored information may pose a threat for consumer privacy, and passive RFID tags cannot be switched off or be put on offline mode.

The main objectives in this study were to depict the state of RFID sector in Finland, to survey the current stage of implementing PIA, and to study user requirements. A total of 33 respondents answered the questionnaire provided for this survey, of which 22 were members of RFID Lab Finland. 39 % of respondents were complete solution providers, 21% equipment suppliers, 12 % tag suppliers, 12 % software/ICT suppliers, 9 % consulting/ research, and 6% other.

According to results, B2B business was most important (74.3 %) customer sector, and three most important customer segments were manufacturing, wholesale/retail, and transportation/storage. 21 % of respondents considered their PIA competence to be at least in high level. Further, PIA seemed to be relatively clearly instructed by the authorities and it is experienced to facilitate business. In general, it seemed that those companies that need to conduct PIA were more familiar with the framework.

Liikenne- ja
viestintäministeriö

Julkaisun päivämäärä
28.2.2012

Julkaisun nimi
Selvitys RFID-toimialasta sekä yksityisyyden suojaa ja tietosuojaa koskevan vaikutusten arvioinnin (PIA) soveltamisesta Suomessa

Tekijät
Karri Rantasila, Antti Permala

Toimeksiantaja ja asettamispäivämäärä
Liikenne- ja viestintäministeriö (LVM)

Julkaisusarjan nimi ja numero Liikenne- ja viestintäministeriön julkaisuja 5/2012	ISSN (verkkojulkaisu) 1795-4045 ISBN (verkkojulkaisu) 978-952-243-289-6 URN http://urn.fi/URN:ISBN:978-952-243-289-6 HARE-numero

Asiasanat
radiotaajuinen etätunnistus (Radio Frequency Identification, RFID), yksityisyyden suojaa koskeva vaikutusten arviointi (Privacy Impact Assessment, PIA), tietoturva, tietosuoja, lähiviestintä (Near Field Communication, NFC)

Yhteyshenkilö Kirsi Miettinen	Raportin kieli Englanti

Muut tiedot

Tiivistelmä

Tämän selvityksen tarkoituksena on kartoittaa RFID-liiketoimintaa Suomessa. Selvityksessä käsitellään erityisesti alan toimijoita, lainsäädäntöä, yksityisyyden suojaa ja tietosuojaa koskevaa vaikutusten arviointikehystä (PIA), sekä käyttäjien käytettävyysvaatimuksia.

Koska RFID-teknologia mahdollistaa langattoman tunnistamisen pitkältäkin etäisyydeltä (jopa 6–8 metriä), on viime vuosina alettu keskustella yksityisyyden suojaa, tietoturvaa ja tietosuojaa koskevan lainsäädännön ja suositusten merkityksestä RFID-liiketoiminnassa. Tätä keskustelua on lisännyt myös hankaluus havaita RFID-infrastruktuuria ja tunnisteiden kuolettamiseen liittyvät näkökulmat.

Tämän selvityksen keskeiset tavoitteet ovat luoda yleiskuva tämän hetkisestä tilanteesta RFID-liiketoimintasektorilla, sekä luodata PIA-kehyksen käyttöä ja käyttäjien vaatimuksia Suomessa. Kyselyyn vastasi 33 henkilöä, joista 22 oli RFID Lab Finlandin jäsenyrityksiä. Vastaajista 39 % edusti kokonaisratkaisujen toimittajia, 21 % laitetoimittajia, 12 % tagitoimittajia, 12 % ohjelmisto/IT-ratkaisutoimittajia ja 9 % konsultointia/tutkimusta. Näiden lisäksi kaksi vastaajaa katsoi edustavansa muuta vastaajaryhmää.

Vastaajista 74,3 % piti B2B-asiakkaita tärkeimpänä asiakassektorinaan, minkä lisäksi yksittäisistä asiakassegmenteistä tärkeimpinä pidettiin valmistavaa teollisuutta, kaupan alaa ja kuljetus/varastointialaa. Vastaajista 21 % katsoi PIA-osaamisensa olevan vähintään korkealla tasolla. Lisäksi PIA-kehys vaikutti olevan selvästi ohjeistettu viranomaisten puolelta ja sen katsottiin edistävän liiketoimintaa. Yleisesti ottaen ne vastaajat, joiden tuli soveltaa PIA-kehystä, myös tunsivat sen paremmin.

FOREWORD

As the present study indicates, the supply and use of RFID applications is only now becoming more widespread in Finland. At present, solutions based on RFID technology can be found in access control systems and public transport travel card systems, for example. Expectations for the future, however, are high, and consumers are likely to come across products and systems using RFID increasingly often.

The purpose of this report is to map out the current situation in the Finnish RFID market. The report explores what type of RFID-based products and services are currently produced and provided in Finland, and what companies providing them are like. Effort is also made to identify problems and obstacles experienced by companies. Furthermore, the report examines how companies perceive their own competence in terms of data protection.

It is hoped that the present study is useful to those interested in Finnish RFID business activities and that it sheds light on the factors that have contributed to the development of the RFID field in Finland. As the report focuses on the current situation in the market, it creates interesting opportunities for following how the market evolves in the future. It can also be considered a basic information package on RFID business in Finland.

The report was prepared by VTT Technical Research Centre of Finland and commissioned by the Ministry of Transport and Communications. The Ministry of Transport and Communications takes no responsibility for any conclusions drawn in the report.

Helsinki, 28 January 2012

Kirsi Miettinen
Director of the Internet Services Unit, Senior Adviser

Table of contents

Table of figures

List of tables

1. Introduction

For a decade, RFID (Radio Frequency IDentification) has been considered as a very promising technology facilitating automated identification and more efficient operations in several industrial and societal domains. As RFID enables remote and wireless automated identification without direct visual connection, it has been expected to be a successor of bar code. (Pilli-Sihvola, Rantasila & Permala 2011)

RFID uses electromagnetic or radio waves to communicate with tags, with the possibility of reading the unique identification numbers or other information stored in them. RFID tags, containing electronic memory and antennae, are small and can take many forms, which is why they are not easy to detect. RFID readers are utilized to read the information stored on RFID Tags. (PIA Framework for RFID Applications 2011)

The utilization of RFID technology relates to privacy issues, as well as it raises various ethical and legal aspects. The European Commission (EC) published its first working document on RFID related data protection issues in 2005. (EC WP 105 2005) In 2009, EU published EU recommendation on RFID applications with expected impact assessment. (EC Recommendation SEC 585 2009) The latest and most comprehensive EU document related to RFID privacy aspects was published in 2011. This document “Privacy Impact Assessment Framework for RFID applications" addresses the requirements of previous publications. (PIA Framework for RFID Applications 2011)

The reason for relatively strong interest of EU on RFID related privacy issues lies in the features of the technology. RFID deployments process information developed through the interaction of tags and readers. The deployments are operated by one or more RFID operator, and connected to back-end systems and networked communication infrastructures. As RFID technology enables identification without direct visual contact at long distances (even 6-8 meters with UHF), it can be considered frightening due to the invisibility. In addition, the tags or readers may not always be detected by the human eye. Also the information that can be collected by utilizing RFID technology can be considered as threat for consumer privacy. Finally, the fact that unlike many other personal devices (e.g. mobile phones), passive RFID tags cannot be switched off or be put on offline mode. (Pilli-Sihvola, Rantasila & Permala 2011)

In order to provide a comprehensive outlook on RFID markets in Finland, Technical Research Centre of Finland VTT has conducted a survey, commissioned by the Ministry of Communications and Transport in Finland. The study was conducted by Karri Rantasila, who was also responsible of the report. Antti Permala and Johan Scholliers have provided their expertise and comments on the work. RFID Lab Finland has supported this work.

The main aspects of the survey cover the profile of RFID sector in Finland, implementation of Privacy Impact Assessment (PIA) framework, and user requirements concerning usability.

The report is divided into six main chapters. Chapter 1 presents the RFID as a technology for identification at the glance, PIA and legislation framework, and current state of RFID markets in global scale. Second chapter discusses the implementation of the study from methodological aspects including data collection, sample, and reliability issues. Chapter 3 depicts the current picture of RFID sector in Finland covering providers, services, customers, and current challenges. In Chapter 4, the current stage of implementing PIA framework in Finland is reflected based on review of legislation framework and survey results. Chapter 5 concentrates on defining user requirements for usability issues. Finally, conclusions are presented in Chapter 6.

1.1 Radio frequency identification

1.1.1 Pivotal Concepts

Some centric concepts need to be defined to facilitate the understanding of privacy impact assessment framework. The list should not be considered to cover technical aspects of RFID, but rather it covers those aspects important for privacy and data protection point of view.

- RFID (radio frequency identification) employs inductive (HF) or radio (UHF) waves to communicate to or from a tag to read the identity of tag or other data stored on it.

- Tag refers either a RFID device having the ability to produce a signal or a device which reflects a signal received from a reader.

- RFID reader means a fixed (e.g. gate/terminal) or mobile (e.g. handheld reader) data capture and identification device using radio or electromagnetic waves to identify tag.

- RFID application processes the data acquired through the use of tags and readers, and is linked to communication infrastructure.

- RFID operator can be natural or legal person, public authority, agency, or any other body, which operates RFID deployment, including controlling personal data.

- Information security refers preservation of the confidentiality, integrity and availability of information.

- Monitoring means any activity carried out for the purpose of detecting, observing, copying or recording the location, movement, activities or state of an individual.

- PIA (Privacy Impact Assessment) is a process whereby a conscious and systematic effort is made to assess the privacy and data protection impacts of a specific RFID deployment with evaluation of necessity of taking appropriate actions to prevent or minimize potential risk.

- PIA Framework identifies the objectives of PIA, the components of RFID deployment, and the common structure and content of PIA Report.

- PIA Report is the document resulting from the PIA process and is available to competent authorities.

1.1.2 Technical aspects

The purpose of this study is not to concentrate on technical aspects of RFID. However, it was considered necessary to briefly discuss on technical issues, and especially standardization issues important for data security, as a background for this study. The main components of RFID system are tags (transponders) and readers (gates, handheld readers etc.). Also databases (middleware) are vital part of the system. The technology is based on unique number of each unit (tag) that can be used to identify it. The tag, formed by an antenna and a chip containing data is attached to the object to be identified. The reader consists of radio frequency transmitter and receiver, an antenna and often a communication interface. The reader is be used to acquire the data stored on the tag. (Finkenzeller 2003) The final part of the system, middleware, is made up of databases for storing information connected to the rest of the system. (McFarlane and Sheffi, 2003)

The current field of different RFID technologies is relatively broad. Radio frequencies, tag types, and methods of coupling vary. RFID tags can be classified into three main types; passive, semi-passive (or semi-active), and active. Passive tags operate without power source, while semi-active and active tags require a power source in the tag. Semi-active tags are examined here together with active tags due to their similar properties. (Pilli-Sihvola, Rantasila & Permala 2011) As tags are carried by the individuals, and can be directly linked to personal data, also privacy issues can be approached from this point of view.

Passive tags utilize the energy of the reader's signal for processing and sending a reply. There are small, passive inductive tags with reading range of few centimeters that are used e.g. for identifying animals. At the other end of the scale are active tags with reading range of over 100 meters. The coupling between the tag and the reader is dependent on the system frequency. The most commonly employed passive technologies are High-Frequency (HF, 125 kHz and 13.56 MHz) and Ultra-High Frequency (UHF, 865–870 MHz). The maximum reading range of the tag depends on the frequency, transmission power, and size and shape of the antennas. Typical applications for systems and tags operating in the 125–134 kHz with a reading range of only a few centimeters include access control, ticketing, and animal identification. Passive UHF tags in the 865–870 MHz range possess longer reading range of 2–6 meters. UHF tags also provide possibility for bulk reading of items with a reading speed of up to 150 tags per second. One field of passive tags is Near Field Communication (NFC, 13.56 MHz) technology, which is mainly used in mobile phones that enable for example payment applications. NFC is yet to be adopted widely in the mobile phone industry, but some manufacturers have indicated that they will equip their phones with NFC capabilities in the near future. (Pilli-Sihvola, Rantasila & Permala 2011)

Active RFID technology has been used for more than a decade mainly for access control applications. Operating frequencies for active tags cover 433.92 MHz, 868–915 MHz, 2.45 GHz and 5.8 GHz. The reading ranges of active tags vary from approximately 10 meters to as long as 500 meters. The 433.92 MHz frequency is important for industries as many identification, monitoring and electronic seal standards are based on it. The 5.8 GHz frequency is mostly used in road traffic applications such as road use charging (i.e. road tolls). Semi-active (or semi-passive) tags are a relatively new on the market. The introduction of these has been facilitated by the arrival of paper-like batteries, which enabled using semi-active tags as normal smart labels with a longer reading range and with more memory than what can be achieved with passive tags. The presence of a power source (i.e. a battery) also makes it possible to store sensor information on active tag's memory. (Pilli-Sihvola, Rantasila, Permala & Scholliers 2011)

As mentioned above, to identify units each of them should have a unique number. This numbering issue has been addressed by two major standardization organizations in two distinct ways. These approaches are 1) the ISO approach, and 2) the EPCglobal/GS1 approach. The ISO and EPCglobal/GS1 models were markedly different during the first years of the 21st century, but recent developments have enabled interoperability between RFID systems based on these two different models. (Pilli-Sihvola, Rantasila, Permala & Scholliers 2011) There are still certain distinct differences between the approaches. ISO (International Standardization Organization) has made the RFID tag self-contained so that all required information is stored within the tag. In the EPCglobal/GS1 model, on the other hand, only the unique reference number is stored in the tag. Related information is retrieved through the Internet, using the reference number as a key to data. This model also allows storing some additional information in the tag. The main followers of ISO approach to the standardization are electronics, automotive and health industries, while the EPCglobal/GS1 model is widely utilized by the retail industry. Several industries (e.g. metal, paper and printing) still utilize proprietary numbering systems. (Permala, Pilli-Sihvola, Rantasila & Scholliers 2011)

1.1.3 RFID for improved Auto-ID

Alongside bar code, RFID has lately become increasingly adapted automated identification (Auto-ID) systems in industrial processes. This is mainly because of decreasing price of passive tags, which is mainly caused by increased volumes that have lowered the production costs per unit. (Rida, Li, Tentzeris, & Mortazawi, 2009) RFID also has numerous advantages compared to traditional barcodes, including higher reading reliability and speed of RFID, as well as no human involvement is necessary at any stage of identification process. Furthermore, the information stored in RFID tags is much more versatile than in case of barcodes that are also more sensible to weather and other environmental conditions. (McFarlane & Sheffi, 2003)

In their thesis Murto and Sipola (2010) state that RFID and NFC technologies have recently reached households. This is rather radical statement but it is though true that the possible deployments of RFID have broaden from traditional industry and supply chain applications significantly. Promising and existing deployments include access control and security deployments, road tolls, payment solutions (including NFC based mobile payment solutions), and smart cards (e.g. electronic ticketing solutions). (Murto & Sipola, 2010)

In Finland one of the most well-known RFID deployments are probably payment solutions for public transport, allowing payments in different transport modes and in different areas with one card (e.g. HSL). Also RFID based ticket solutions have become more common in recent years for example in sport events or sporting facilities. Murto and Sipola also mentioned the concept of “city card” which allows combining the access of different public services (e.g. swimming halls) in one smart card. Also new biometric passports contain RFID chip. In addition, international examples of RFID deployments for consumers include fuel station payment cards, as well as several large credit card companies have launched first payment card operating without physical contact. (Murto & Sipola 2010)

Electronic ticketing solutions like smart cards and NFC based payment offer possibilities to increase customer friendliness, reduce fare evasion, lower fare collection costs, apply innovative pricing solutions, and improve efficiency of public transport systems. (Hobbs & Streeting, 2009; UITP Position Paper, 2007)

In general, several incentives of RFID implementation can be identified. Deployments are justified by improved operational efficiency, enhanced cooperation with the partner network, added value for the customer, improvements of market position, or by cost savings. Especially in industrial sector, improved accuracy, less throughput time, and decreased personnel, are main motivators of RFID deployment. RFID can support achieving these goals, but requires also the development of processes (Permala & Scholliers, 2008). When RFID is fully deployed and integrated into the other systems it also facilitates several other functions like purchasing, production processes, inventory control, quality control, and inter-organizational flow of materials. (Roh, Kunnathur, & Tarafdar, 2009) In future, the wide-scale deployment of RFID may also enable more sophisticated solutions such as the Internet of Things (CERP 2008).

Even the benefits of RFID deployments are agreed, it is difficult to present general benefits in monetary terms. Some authors have quantified the savings generated by RFID on a case-by-case basis (see e.g. (Granqvist, Permala, & Scholliers, 2007) and Kärkkäinen (2003)). For example Kärkkäinen estimated that annual savings for a large British supermarket chain were 8.5 million pounds (Kärkkäinen, 2003). Almost half of these savings resulted from reduced stock losses.

Despite of widely agreed benefits and potential of RFID, there are also several critical issues in RFID implementation. The breakthrough of RFID in business practices has been expected for several years, but due to some major barriers, mainly related to information sharing and interoperability standards, it has not been seen yet. Some years ago, major obstacles of RFID deployments were the price of tags and performance near metals. Prices of tags have come down, as well as the performance of tags has increased considerably even when attached to metal. Still, further challenges and impediments of successful implementation of RFID systems, recognized in previous research include ownership transfer, computing bottlenecks, read errors, cost-benefit issues, and risk of obsolescence. (Kapoor, Zhou, & Piramuthu, 2009)

Serious criticism has also been addressed towards security issues of RFID in systems (Zuo, 2010) as the system should be designed with sufficient security to prevent unauthorized use and protect data. Additional problems are caused by the different frequencies used for RFID worldwide (Kapoor, Zhou, & Piramuthu, 2009). The content of tag data like identification code (e.g. EPC), parcel information, addresses, receipts, needs to be agreed. Finally, the interoperability of different tags, readers, protocols and interfaces is a major issue as it benefits the supply chain actors. Furthermore, Global Data Synchronization (GDS) is a prerequisite for RFID-based automatic identification, and a uniform coding or numbering system must be used by all partners. (Granqvist, et al., 2007)

The importance of efficient information management grows as the number of tags increases. The data needs to be handled and stored in quick and efficient manner, as well as information must be timely and easily available to all who need it (transparency). While mapping critical future challenges of RFID in next five years, Frost & Sullivan (2011) addressed the lack of end-user knowledge, reluctance of companies to experiment due to the risks involved. Also the lack of standards and inadequate infrastructure are also considered as restraints on the RFID market. (Frost & Sullivan 2011) The mostly utilized RFID deployment in EU is person identification and access control, which is one reason why the European Commission has initiated several activities related data protection and privacy issues since 2005. These initiatives are further discussed in next subchapter.

1.2 Privacy impact assessment framework

1.2.1 Overview of privacy related regulations in EU

Four essential EC directives concerning privacy and data protection issues can be identified. As these form the background for PIA, the main aspects are briefly discussed below. For more comprehensive information, reader may refer the references provided for each regulation. In addition, some organizations have published downloadable PIA tools (see for example GS1 EPC/RFID Privacy Impact Assessment Tool)

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data was published in 1995. Directive is European level reference text on the protection of personal data, which sets up a regulatory framework seeking to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union. The directive sets limits on the collection and use of personal data, as well as it demands each Member State to set up an independent national body responsible for the protection of these data. (Directive 95/46/EC 2002)

Directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (1999) establishes a regulatory framework for the placing on the market, free movement and putting into service of radio equipment and telecommunications terminal equipment in the Community. (Directive 1999/5/EC 1999)

The Charter of Fundamental Rights of the European Union (2000) sets out a single text covering the whole range of civil, political, economic and social rights of European citizens and all persons resident in the EU. The rights are divided into six sections in the Chapter: dignity, freedoms, equality, solidarity, citizens' rights, and justice. Privacy and data protection issues are addressed most of these sections in general level, but especially citizens' rights and justice sections sets some important principles from privacy point of view. (The Charter of Fundamental Rights of the European Union 2000)

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002) address the requirements to ensure that users have a right to privacy. The Directive contains crucial provisions to ensure that users are abel to trust the services and technologies they use for communicating electronically. (Directive 2002/58/EC 2002)

1.2.2 EC Recommendation SEC 585 2009

In 2005, EC established a stakeholder group that involved both industry players and privacy rights organizations. The aim of this group was to compromise on how to leverage the potential of RFID, while still respecting peoples' privacy. The result was published in EC's Communication in 2007 on RFID, followed by a *Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification* in 2009. This recommendation was further elaborated "PIA regulation" to be implemented in member countries. This is further discussed in following subchapter

The recommendation introduced several measures to enhance awareness for privacy and data protection practices and requested dedicated actions by Member States and the industry applying RFID based on consultation of European Data Protection Supervisor. During the consultation, following points were addressed (EC Recommendation SEC 585 2009):

- RFID technology enables the processing of data, including personal data, over short distances without physical contact or visible interaction between the reader or writer and the tag, such that this interaction can happen without the individual concerned being aware of it.

- RFID applications hold the potential to process data relating to an identified or identifiable natural person, a natural person being identified directly or indirectly. They can process personal data stored on the tag such as a person's name, birth date or address or biometric data or data connecting a specific RFID item number to personal data stored elsewhere in the system. Furthermore, the potential exists for this technology to be used to monitor individuals through their possession of one or more items that contain an RFID item number.

- Because of its potential to be both ubiquitous and practically invisible, particular attention to privacy and data protection issues is required in the deployment of RFID. Consequently, privacy and information security features should be built into RFID applications before their widespread use (principle of 'security and privacy-by-design').

- RFID will only be able to deliver its numerous economic and societal benefits if effective measures are in place to safeguard personal data protection, privacy and the associated ethical principles that are central to the debate on public acceptance of RFID.

- Member States and stakeholders should, especially in this initial phase of RFID implementation, make further efforts to ensure that RFID applications are monitored and the rights and freedoms of individuals are respected.

- The Commission Communication of 15 March 2007 'Radio Frequency Identification (RFID) in Europe: Steps towards a policy framework' announced that clarification and guidance would be provided on the data protection and privacy aspects of RFID applications through one or more Commission Recommendations.

- The rights and obligations concerning the protection of personal data and the free movement of such data, as provided for by 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 on the free movement of such data and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on privacy and electronic communications are fully applicable to the use of RFID applications that process personal data.

- The Opinion of the European Data Protection Supervisor provides guidance as to how to handle products that contain tags which are provided to individuals and calls for privacy and security impact assessments to identify and develop 'best available techniques' to safeguard the privacy and security of RFID systems.

- RFID application operators should take all reasonable steps to ensure that data does not relate to an identified or identifiable natural person through any means likely to be used by either the RFID application operator or any other person, unless such data is processed in compliance with the applicable principles and legal rules on data protection.

- The Commission Communication of 2 May 2007 on 'Promoting Data Protection by Privacy Enhancing Technologies (PETs) sets out clear actions to achieve the goal of minimizing the processing of personal data and using anonymous or pseudonymous data wherever possible by supporting the development of PETs and their use by data controllers and individuals.

- The Commission Communication of 31 May 2006 'A Strategy for a Secure Information Society — Dialogue, partnership and empowerment' acknowledges that diversity, openness, interoperability, usability and competition are key drivers for a secure Information Society, highlights the role of Member States and public administrations in improving awareness and in promoting good security practices, and invites private-sector stakeholders to take initiatives to work towards affordable security certification schemes for products, processes and services addressing EU-specific needs, in particular with respect to privacy.

- The Council Resolution of 22 March 2007 on a strategy for a secure information society in Europe invites Member States to give due attention to the need to prevent and fight new and existing security threats to electronic communications networks.

- A framework developed at Community level for conducting privacy and data protection impact assessments will ensure that the provisions of this Recommendation are followed coherently across Member States.

- The Commission will ensure the development of guidelines at Community level on information security management for RFID applications, building on existing practices and experiences gained in Member States and third countries. Member States should contribute to that process and encourage private entities and public authorities to participate.

- An assessment of the privacy and data protection impacts carried by the operator prior to the implementation of an RFID application will provide the information required for appropriate protective measures. Such measures will need to be monitored and reviewed throughout the lifetime of the RFID application.

- In the retail trade sector, an assessment of the privacy and data protection impacts of products containing tags which are sold to consumers should provide the necessary information to determine whether there is a likely threat to privacy or the protection of personal data.

- The use of international standards, such as those developed by the International Organisation for Standardisation (ISO), codes of conduct and best practices which are compliant with the EU regulatory framework can help to manage information security and privacy measures throughout the whole RFID-enabled business process.

- RFID applications with implications for the general public, such as electronic ticketing in public transport, require appropriate protective measures. RFID applications that affect individuals by processing, for example, biometric identification data or health-related data, are especially critical with regard to information security and privacy and therefore require specific attention.

Based on these issues described above, EC Recommendation SEC 585 aims at ensuring full respect for the privacy and protection of personal data, by providing guidance for RFID deployments in a lawful, ethical, socially and politically acceptable way. Furthermore, the recommendation provides guidance on measures to be taken for the deployment of RFID to ensure that national legislation will implement Directives 95/46/EC, 99/5/EC and 2002/58/EC. Key aspects of the recommendation are summarized below. (EC Recommendation SEC 585 2009)

Privacy and data protection impact assessments. Member States should ensure that industry, in collaboration with relevant administrative stakeholders, develops PIA framework. Member States should also ensure that operators pursue to Directive 95/46/EC, including:

- Conducting an assessment of the implications of the application implementation for the protection of personal data and privacy, whether the application could be used to monitor an individual. The level of the assessment should be appropriate to the privacy risks possibly associated with the application.

- Taking appropriate technical and organizational measures to ensure the protection of personal data and privacy.

- Designating person/persons responsible for reviewing the assessments and the continued appropriateness of the technical and organizational measures to ensure the protection of personal data and privacy.

- Making the assessment available to the competent authority at least six weeks before the deployment of the application.

- Implementing the provisions in accordance PIA.

Information security. Member States should support the Commission in identifying applications raising information security threats. Further, Member States should ensure that operators, together with national competent authorities and other organizations, develop new schemes or apply existing schemes (e.g. certification or operator self-assessment), in order to demonstrate that an appropriate level of information security and protection of privacy is established.

Information and transparency on RFID use. Member States should ensure that operators develop and publish a concise, accurate and easy to understand information policy (in accordance with Directives 95/46/EC and 2002/58/EC) for each of their applications. Policy should include:

- Identity and address of the operators.
- Purpose of the application.
- Specification of data to be processed by the application, especially if personal data will be processed, and whether the location of tags will be monitored.
- Summary of the PIA.
- Potential privacy risks relating to the use of tags in the application, as well as the measures, which individuals can take to mitigate these risks.

It is responsibility of Member States to ensure that operators take above mentioned steps to inform individuals of the presence of readers with a common European sign. The sign should specify the operator and its contact information.

RFID applications used in the retail trade. As retail is one of the main concerns related to data privacy operators should also inform individuals of the presence of tags that are placed on or embedded in products. It should be also considered whether tags placed on (or embedded in) products sold to consumers through retailers, who are not operators, posses a likely threat to privacy or the protection of personal data. The tags should be deactivated (stops those interactions of a tag) or removed at the point of sale unless consumers give their consent to keep tags operational. Consumers should also be able to verify that the deactivation or removal is effective. However, tags should be deactivated or removed only if PIA concludes that tags that are likely threat to privacy or the protection of personal data. There are also Finnish examples in field of applying RFID in retail business. One of the broadest ones is deployment of Naisten Pukutehdas, which has employed RFID in shop floor solutions.

Awareness raising actions. Members States, industry, EC, and other stakeholders should take appropriate measures to inform and raise awareness of the potential benefits and risks associated with the use of RFID technology (specific attention should be given to information security and privacy aspects). Also examples of good practices and measures (e.g. pilots) in the implementation of RFID applications should be identified and communicated to raise awareness.

Research and Development. Member States should cooperate with industry and other relevant stakeholders, and EC to stimulate and support the introduction of the ‘security and privacy by design’ principle at an early stage in the development of RFID applications.

Follow-up. Member States should take measures to bring this Recommendation to the attention of all relevant stakeholders involved in the design and operation of RFID applications. In addition, Member States should inform the Commission at the latest 24 months following the publication of this Recommendation of actions taken in response to this Recommendation. Currently, Finland has provided its industry commentary concerning the proposed PIA framework (Finland commentary 00327/11/FI). Finally, within three years after the publication of the Recommendation, EC will provide a report on the implementation of this Recommendation including its effectiveness and its impact on operators and consumers. This issue is also linked to purpose of this study.

1.2.3 PIA Framework for RFID applications

The Recommendation of EC discussed in previous subchapter, established a requirement for the endorsement of an industry-prepared framework for Personal Data and Privacy impact assessments (PIA) for RFID Applications. The benefits of conducting PIAs for RFID operator include following (PIA Framework for RFID Applications 2011):

- Establish and maintain compliance with privacy and data protection laws and regulations.
- Manage risks to its organization and to users of RFID applications.
- Provide public benefits of RFID Applications while evaluating the success of privacy and to develop the process.

The PIA process is based on a privacy and data protection risk management approach, focusing on the implementation of the EC Recommendation and consistent with the EU legal framework. The process is designed to help operators to uncover and assess privacy risks of RFID deployments, and to document the actions implemented to address those risks. Framework provides guidance to operators on the risk assessment methods with introduction to mitigate any likely data protection or privacy impact in an efficient, effective and proportionate manner. (PIA Framework for RFID Applications 2011)

As the responsibility of conducting PIA belongs to RFID operator, it should have own internal procedures to support the execution of PIAs. These procedures include following aspects (PIA Framework for RFID Applications 2011):

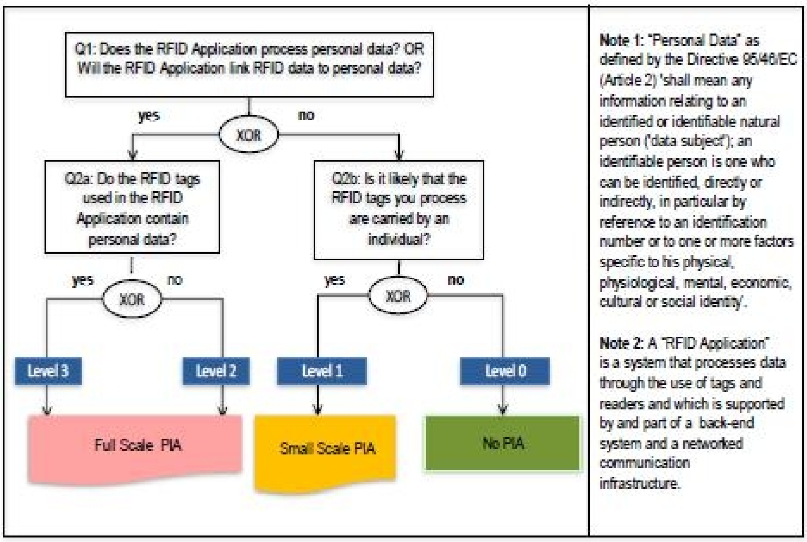
- Scheduling of the PIA process (report available to the competent authorities at least six weeks before deployment).
- Internal review of the PIA process and PIA Reports for consistency with other documentation related to the RFID Application.
- Compilation of supporting artifacts (e.g. results of security reviews) as evidence that the operator has fulfilled all of the applicable obligations.
- Determination of the persons and/or functions within the organization with authority for relevant actions during the PIA process.
- Provision of criteria for how to evaluate and document whether deployment is consistent with the framework.
- Consideration/Identification of factors that would require a new or revised PIA.
- Stakeholder consultation, collecting opinions and feedback from relevant stakeholders related to application and PIA.

RFID operators must conduct a PIA for each RFID application, although they may create one PIA report in case of several related RFID deployments (potentially in the same context or at the same premises), if the boundaries and differences of the applications are explicitly described in the report. In addition, if operators reuse one application in the same way for multiple products, services or processes, they may create only one PIA report. The PIA process consists of two phases (PIA Framework for RFID Applications 2011):

- Initial Analysis Phase, during which the operator determine whether a PIA is required or not and whether it'll be full or small scale PIA.

- Risk Assessment Phase, which outlines the criteria and elements of full and small scale PIAs.

To conduct the initial assessment phase, an operator needs to go through the decision tree depicted in Figure 1, which helps operator to determine whether and to what extent a PIA is needed for the RFID Application in question. The results of initial analysis must be documented and made available to data protection authorities upon request. (PIA Framework for RFID Applications 2011)


Q1: Does the RFID Application process personal data? OR Will the RFID Application link RFID data to personal data?
yes
XOR
no
Q2a: Do the RFID tags used in the RFID Application contain personal data?
Q2b: Is it likely that the RFID tags you process are carried by an individual?
yes
XOR
no
yes
XOR
no
Level 3
Level 2
Level 1
Level 0
Full Scale PIA
Small Scale PIA
No PIA

Note 1: "Personal Data" as defined by the Directive 95/46/EC (Article 2) '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'.

Note 2: A "RFID Application" is a system that processes data through the use of tags and readers and which is supported by and part of a back-end system and a networked communication infrastructure.

Figure 1 PIA Decision tree

The goal of risk assessment phase is to identify the privacy risks caused by a deployment and to document how these risks are pro-actively mitigated with technical and organizational control. It is recommended that risk assessment phase is finalized before final decisions on RFID architecture are taken. Risk assessment process considers the risks of the RFID deployment in terms of likelihood and magnitude of consequences. Four steps can be identified (PIA Framework for RFID Applications 2011):

1. Characterization of application gives a comprehensive picture of the deployment, its environment and system boundaries. In addition, the design, interfaces with other systems, and information flows and structures are described (data flow diagrams are recommended to visualize information flows).

2. Identification of risks phase identifies and lists how deployment could threaten privacy and estimates the magnitude and likelihood of possible risks. The goal is to identify conditions and risks (related to the RFID components, its operations, and data sharing and processing environment) that may threaten or compromise

personal data. In addition, PIA requires a relative quantification of these risks (low, medium or high), which is why the operator should consider:

- The significance of a risk and the likelihood of its occurrence.
- The magnitude of the impact should the risk occur.

A primarily concern is that RFID tags could be used for the profiling and/or tracking of individuals. Related to this several aspects of especially in consumer retail needs to be taken in to account (see 1.2.2).

3. Identification and Recommendation of Controls. The goal of this step is to analyze the controls (technical like encryption or nontechnical like operational procedures) that have been implemented or planned, in order to minimize, mitigate or eliminate the identified privacy risks. There can also be natural controls created by the environment (for example, if there are no readers installed because there is no business case for it, then naturally there is also no risk).

4. Documentation of Resolution and Residual Risks. After completing the risk assessment, the PIA report should be issued with any further remarks concerning risks, controls, and residual risks. RFID deployment is approved for operations once the PIA Process has been completed, relevant risks identified and appropriately mitigated, with appropriate internal reviews and approvals. If deployment is not approved for operations in its current state new PIA needs to be completed after improvements in order to reach an approvable state.

1.2.4 Current legislation in Finland

According Tancock, Pearson and Charlesworth (2010) there was no collaborating evidence or material related to PIA within Finland to be found. However, authors stated that Finland had discussed the possibility of utilizing PIA based on the models found in Canada, Australia, and New Zealand (Tancock, Pearson and Charlesworth 2010). Also PIAw@tch - the Privacy Impact Assessment observator stated that Finland is “one of the only European countries to contemplate PIAs” (PIAw@tch - the Privacy Impact Assessment observatory, Finland).

Finland has also adopted several supranational privacy regulations including Directive 2002/58/EC, The Charter of Fundamental Rights of the European Union, Directive 1999/5/EC, Directive 95/46/EC, and supranational PIA regulation (Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification 2011). (PIAw@tch - the Privacy Impact Assessment observatory, Finland)

In general there are also several legislations in Finland that constitutes privacy and data protection related issues. Section 10 of the Constitution of Finland (The right to privacy) states that: "Everyone's private life, honour and the sanctity of the home are guaranteed”. The Personal Data Protection Act (1999) made Finnish law consistent with the EU Data Protection Directive and introduced the concepts of informed consent and self-determination into Finnish law. Telecommunications privacy is regulated by the Protection of Privacy and Data Security in Telecommunications Act, which came into force in 2000. The law covers all telecommunications and a new version of the law is currently being drafted under to transpose the EU Privacy and Electronic Communications Directive. On 2003, the Act on Electronic Signatures, went into effect with a purpose to promote the use of electronic signatures and the provision of products and services related to them as well as to promote data protection and data security of electronic commerce and electronic communication. A specific law on Data Protection in Working Life was entered into force in 2001 covering for example surveillance devices. (Privacy

International, Finland) Additionally, there may also be other relevant legislations (e.g. Consumer Protection Act 2005, and Act on the Protection of Privacy in Electronic Communications 2004) but it is not relevant to discuss these more comprehensively as PIA framework is considered as its own recommendation.

1.3 RFID business

1.3.1 Current situation in global scale

In global context, the awareness of RFID technology is highest in North America and Europe. The difference in deployments between these two areas lies in scale; whereas North America has several high-volume deployments in progress, Europe is more active in pilot deployments. In other continents, South America has the most future growth potential, while Asia Pacific is seen as the region with the highest growth rates. Not surprisingly, Africa has the lowest level of RFID penetration. (Frost & Sullivan, 2011)

Despite of improvements, RFID technology is still relatively marginally adopted by companies in Europe (Permala, Pilli-Sihvola, Rantasila & Scholliers 2011). According to Eurostat 3 % of EU27 enterprises used RFID in January 2009. The top adoption rates were experienced in Netherlands (9 %), Finland (8 %), Germany, Spain, Austria and Slovakia (all 4 %). Correspondingly, the lowest shares of utilizing RFID were Greece, Cyprus and Romania (all 1 %).

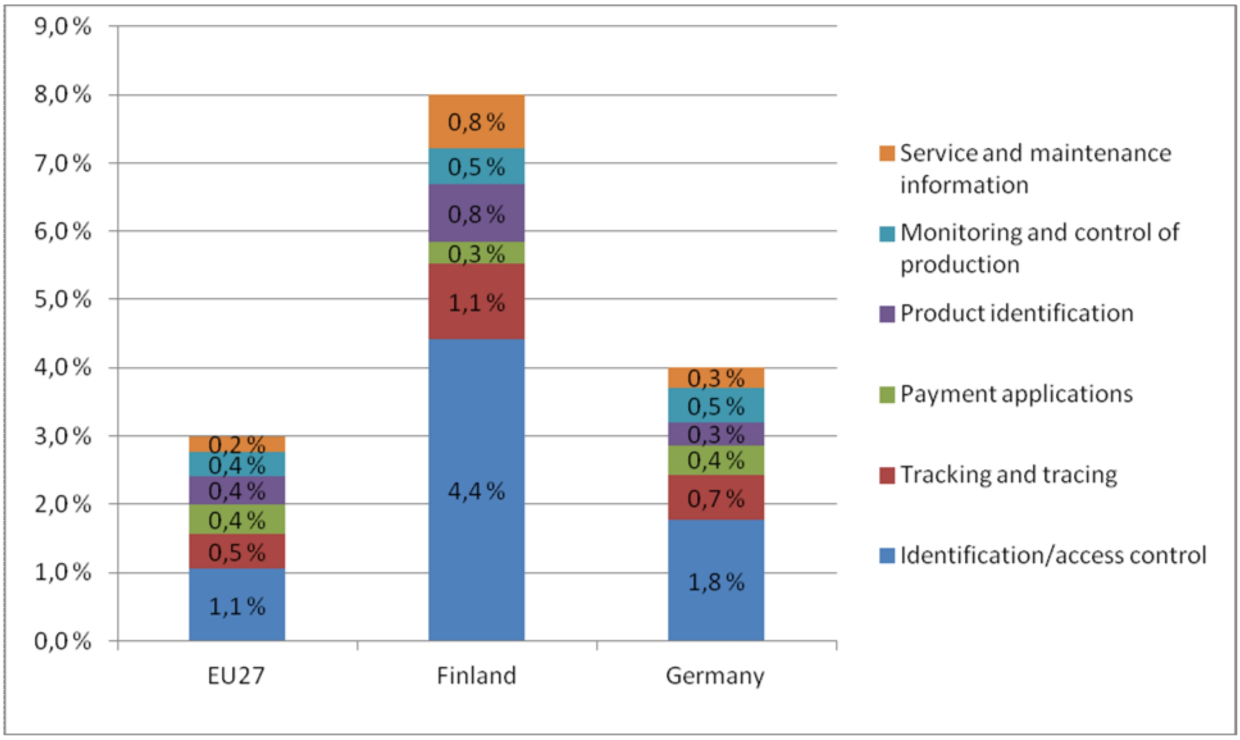


Figure 2 Use of RFID by purpose (% of enterprises using RFID, multiple answers possible) in EU-27, Finland and Germany, 2009 (Permala, Pilli-Sihvola, Rantasila, Scholliers 2011)

The main usage of RFID in EU27 is related to personnel monitoring or access control (56 %), followed by tracking and tracing (29 %), which is the second biggest use in all presented areas. Other deployments include payment applications (25 %), product identification (24 %), monitoring and control of production (21 %), and service/maintenance information & information/asset management (15 %). Country specific results of RFID deployments are presented in Table 1. (Eurostat Newsletter 12/2010)

Table 1 RFID in Europe 2009 by purpose (data source Eurostat Newsletter 12/2010)

	By purpose (% of enterprises using RFID, multiple answers possible)N/A						
	Enterprises using RFID, % of all enterprises	Person Identification or access control	Supply chain and inventory tracking and tracing	Payment applications (e.g. tolls, public transport)	Product identification (e.g. theft control	Monitoring and control of industrial production	Service and maintenance information management, asset management
EU27 average	3	56	29	25	24	21	15
Belgium	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Bulgaria	2	71	18	13	24	16	13
Czech Republic	3	83	13	7	12	13	14
Denmark	2	54	21	30	22	17	21
Germany	4	63	22	13	9	16	8
Estonia	2	87	18	22	26	23	20
Ireland	2	33	43	32	38	21	20
Greece	1	11	30	10	57	26	12
Spain	4	40	44	30	31	34	24
France	3	44	34	33	49	23	13
Italy	3	38	33	48	25	24	13
Cyprus	1	53	20	7	41	27	20
Latvia	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Lithuania	3	35	43	39	43	25	52
Luxembourg	2	70	32	22	19	23	21
Hungary	2	59	22	4	19	11	15
Malta	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Netherlands	9	78	18	7	11	13	7
Austria	4	57	16	44	15	10	6
Poland	3	74	N/A	N/A	28	29	N/A
Portugal	2	46	N/A	N/A	N/A	N/A	N/A
Romania	1	48	20	17	27	25	18
Slovenia	3	51	13	28	19	14	18
Slovakia	4	70	22	4	23	10	12
Finland	8	82	20	5	15	9	14
Sweden	2	71	22	17	15	23	14
United Kingdom	2	52	36	20	28	14	27
Croatia	4	48	22	39	18	12	14
Norway	1	63	28	17	21	23	24

1.3.2 Finnish cases

As presented in figures and tables above, Finland is one of the leading European countries in RFID deployments. Two examples of Finnish RFID deployments, one in manufacturing (ABB) and one in retail (Naisten Pukutehdas), are briefly described below.

ABB Drives' manufacturing plant in Pitäjänmäki has utilized RFID solutions since 2004. The first RFID deployments were related to tracking of transport plywood boxes used in raw material supply. This implementation, which is still in use, was based on reading of tagged boxes in both suppliers' premises and ABB's factory. RFID readers in loading areas recorded all incoming and outgoing shipments. When moved to the loading dock, empty raw material boxes triggered an order to supplier automatically. Correspondingly, as supplier fulfilled the order, an electronic shipping document was automatically generated. Goods were automatically identified and registered in ABB's ERP system via RFID portal, which removed the need of traditional paper shipping documents. The pilot project was executed with selected suppliers as a part of Tekes' ELO (e-Business Logistics) programme. ABB mounts tag on the pallet or box as soon as a drive is manufactured, enabling gates to verify if the products are going to the correct vehicle. The deployment provides several benefits that increase productivity and efficiency. These benefits include real-time tracking, decreased of needed storage capacity in consolidation area, and reduced errors in shipments. In practice deployment eliminates the possibility of incorrect shipment, increases transparency, reduce lead times, improve quality of goods traffic data, as well as it releases capital for investments. (ABB's Press Release 2005; RFID Lab Finland Case Bank/Case ABB; Wessel 2009; Permala, Pilli-Sihvola, Rantasila & Scholliers 2011)

Naisten Pukutehdas (NP) is Finnish-based fashion manufacturer and retailer established in 1919. Their retail network of NP consists of 11 shops in Finland and two in St. Petersburg, Russia. (NP company overview) NP piloted RFID widely in 2007 in order to improve the visibility from manufacturing plants all the way to the shop floors of retail stores. Pilot succeeded to provide 75 % time savings on receiving goods and other distribution center processes, which encouraged NP to tag all items and adapt RFID in store environment in the latter part of 2008. RFID enabled the "intelligent store concept", driven by interactive experience (e.g. smart fitting rooms with touch screens providing additional information on products, suggesting accessories, and enabling customers to order different products or sizes straight to the fitting room), provides shoppers an opportunity to consider a wider range of products, which eventually should increase sales and revenues. RFID also allowed the automation of routines in in-store product handling resulting 25 % savings. Furthermore, it was reported that as personnel had more time for customer service, the sales went up by 18 %. Since autumn 2009, RFID deployment has expanded to facilitate automated shipment receiving, intelligent dressing spaces, interaction points in shops, checkouts and anti-theft solutions, and inventory management. For NP, RFID deployment has delivered improved visibility of the supply chain, improved manufacturing and inventory management, and decreased logistics costs. NP also discovered reduced shrinkage and theft levels. It was also agreed that retail level RFID deployment had positive effect on the reduction of out-of-stock and out-of-shelf situations, customer service and customer satisfaction, accuracy of inventory levels, and the replenishment process in general. (RFID Lab Finland/Case NP; Swedberg, 2008, NP Smart Clothing Store)

There are also several other examples of Finnish RFID deployment projects and pilots in several different industries and contexts. Further examples can be found for example from the Case Bank of RFID Lab Finland.

1.3.3 Future outlook

The development in the implementation of RFID has followed a typical progression of an evolving technology. Three phases may be identified in this development: the first phase of enthusiasm was realized in 2004 and 2005. It was followed by a period of disillusionment somewhere between 2006 and 2008. After 2008 RFID has moved into the present situation, where understanding of the technology's relevance and its role in the market or domain is better understood. (Bendavid & Cassivi, 2010)

EU-funded BRIDGE project forecasted the number of tags purchased annually in 2007. According the study, the annual market volume of passive RFID tags in Europe will be over 86 billion in 2022. In same year, the total number of RFID readers deployed will be over six million in Europe. Furthermore, it was predicted that in 2012 2 % of all retail items will be tagged. The results of forecast are more comprehensively illustrated in Table 2. (European passive RFID Market Sizing 2007-2022, 2007)

Table 2 Forecast of passive RFID deployments in Europe (data source European passive RFID Market Sizing 2007-2022, 2007)

	2012	2017	2022
Total number of tags purchased annually (millions)	3 220	22 400	86 700
Total number of locations with RFID readers	30 710	144 000	453 000
Total number of RFID readers deployed	176 280	1 161 800	6 268 500

Retail and consumer goods are predicted to remain largest RFID tags and readers with two-thirds of the total volume. The main volumes are coming from item-level tagging. These issues further address the importance of data protection and privacy concerns. A forecast for retail & consumer goods RFID deployments is presented in Table 3.

Table 3 Passive RFID tags and readers for consumer and retail goods in Europe (data source European passive RFID Market Sizing 2007-2022, 2007)

	2012	2017	2022
RFID Tags (Millions)			
On food items	520	5 200	31 700
On non-food items	960	5 000	12 400
On cases	760	3 300	11 500
On pallets	40	200	500
Total RFID tags	2 270	13 700	56 100
Locations with RFID readers	11 590	59 900	206 600
Total number of RFID readers	70 570	502 700	3 440 500

Most prominent growth opportunities for RFID deployments are provided by market segments like retail, commercial services, electronics, health care, and pharmaceuticals. Possible applications include asset and people tracking, ticketing, payment, sensing/monitoring, and access control/security/ID. (Wimmer & Nathanson 2010)

According to a Finnish survey conducted in 2006, almost 50 percent of large Finnish manufacturing and trading enterprises that operate internationally expected that they will implement RFID technology in the next five years (Naula, Ojala, Solakivi, Takalokastari, Rantanen, Kalske, Engblom, Häkkinen, Essén, Töyli & Stenholm 2006). Similar wide-scale RFID adoption in the near future was also forecasted in the RFID roadmap published in 2006 (Permala, Scholliers, & Granqvist, 2006).

At the moment, it seems that adoption of RFID deployments has not been as rapid as predicted in 2006. According Finland State of Logistics 2009 survey, deployment of RFID is still in modest level. This applies manufacturing and retail sector, as well as logistics service providers. (Solakivi, Ojala, Töyli, Halinen, Lorentz, Rantasila, Naula 2009)

2. Implementation of the study

This chapter discusses the methodological aspects of conducting the survey, covering target group and sample, as well as data collection methods. Also the reliability of the study is considered.

2.1 Target group and sample

The target group of the survey was RFID service providers, operating in Finland. These were further divided into several subcategories based on their respective service and product portfolio. As this was also one output of the study, it is further discussed in Chapter 3.

Invitation to survey was sent to 202 recipients by email. The list of relevant recipients was retrieved from two main sources: members of RFID Lab Finland, and several business databases. The preference was given to members of RFID Lab Finland, meaning that if recipient existed in both lists, the link to survey was sent via mailing list of RFID Lab Finland. The approach ensured the broad coverage of the survey and including all relevant respondents.

RFID Lab Finland is public, non-profit association, which member companies and organizations include all the major players in the RFID industry in Finland. Their objective is to enhance the business development based on Finnish knowhow in the area of automatic identification and especially in RFID technology. (RFID Lab Finland) 146 out of 202 recipients (73 %) received a link to survey via mailing list of RFID Lab Finland.

Other source of potential recipients consists of free of charge and commercial business databases. Following commercial databases were exploited under the license of VTT: Fonecta Profinder B2B (domestic), Kompass (global). The contacts retrieved from these commercial databases were complemented with additional searches in non-commercial databases like Kauppalehti company search. Only one invitation and one reminder was sent to all companies.

Sample was categorized based on two background variables of the survey. First of these background variables was turnover, according which the companies were divided into four categories. The turnover categories in this survey were:

- Large companies (turnover over 50 MEUR)
- Medium-sized companies (turnover 10-50 MEUR)
- Small companies (turnover 2-10 MEUR)
- Micro companies (turnover 0-2 MEUR)

If RFID business was only a part of group's business, the respondent was asked to quote turnover of RFID business only. Second background variable employed was the main product/service of company's RFID business. The options for respondent were:

- Software/ICT
- Complete solution provider
- Equipment supplier
- Tag supplier
- Consulting/research
- Other (please specify)

The both questions concerning background variables were obligatory. In latter question, two aswers in other category were received; pallet manufacturer, and card supplier.

2.2 Data collection

In practice, the data for the survey was collected by web-based surveying program Webropol. The link of the survey was sent 202 recipients in beginning of November 2011, followed by a reminder one week later for those didn't respond.

In total 33 responses for survey was received. Thus, the response rate was 16,3 %. Most respondent were considered as micro companies (64 %). Share of small companies was 18 %, followed by large companies (12 %), and medium-sized companies (6 %). The absolute number of companies in each turnover category is presented in Figure 3.

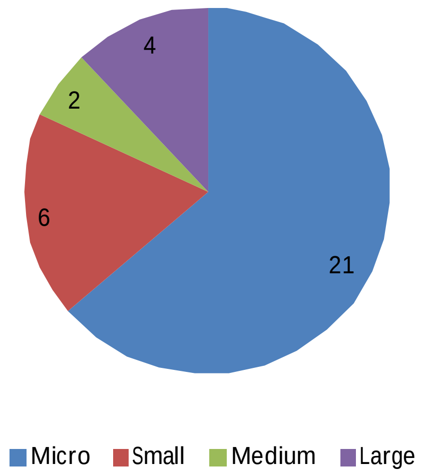


Figure 3 Survey respondents based on company size (n=33)

2.3 Reliability of research

Reliability refers the repeatability, the ability of research to generate non-random results despite the time and person conducting the research (McNeill & Chapman 2005, 9). In general, it can be agreed that larger samples have higher reliability than smaller ones. (Hirsjärvi, Remes & Sarjavaara. 1997, 216; Heikkilä 2000, 30, 187)

Considering the reliability of this survey, the reliability of the collected data is in centre of interest. The empirical data is collected with web-based online survey, which has substantial technological and methodological advantages like short response time and convenience for user. (Kotzab, Seuring, Müller & Reiner 2005) The questionnaire for survey was created by researchers of VTT with extended experience of conducting surveys. Further, the questionnaire set was pre-reviewed by the experts of client and RFID Lab Finland. The questionnaire also included some compulsory questions, in order to ensure sufficient background information. Problems related to questionnaires are usually caused by misinterpretation, or even misunderstanding of question. These problems very mitigated by reviewed of experts and user-friendly web interface. Considering the sample size, it can be stated that 30 is generally mentioned as minimum for some statistical tests. This limit has been exceeded in this study, and as this survey is mainly descriptive, the need for applying statistical methods is relatively low. Thus, the results are based on questionnaire, not on quantitative analysis.

3. RFID sector

As discussed above, to address the questionnaire all relevant recipients, member register of RFID Lab Finland was utilized. In addition, to further increase the coverage, company search was made to databases. Based on number of companies received the questionnaire, there are around 200 companies in Finnish RFID sector. The results presented in this chapter are based on survey conducted among 33 of these companies.

3.1 Service providers

One purpose of the survey was to categorize the companies from the viewpoint of different RFID services provided. In addition, it was surveyed how companies turnover is generated from different geographical areas.

Preliminary categorization of RFID service providers was categorized by the research team prior conducting the survey. Based on this a six-scale categorization was created:

- Complete service providers. These are integrators that provide “one-stop-shop” for customers. They do not necessary produce all the services and equipments by themselves but from customer’s perspective they are the sole point of contact. Are able to deliver complete solutions from planning to training and maintain the deployment.

- Equipment suppliers. The main business of equipment suppliers is to manufacture, and/or sell the RFID readers (i.e. gates and handheld readers) and printers etc. necessary equipments that not fall under other categories. Also installing equipments may be included to their provision.

- Tag suppliers. Their main product is manufacturing and/or selling tags.

- Software/ICT. These companies provide system integration and/or software services related to RFID deployments. Their main product is software or ICT that are needed to employ deployment.

- Consulting/research. Providers of RFID knowhow, whose main service is not to implement RFID deployment, but rather provide produce background information for this.

- Other. Those companies, who do not consider themselves to belong any other category.

The categorization was drafted before the survey in order to provide a starting point for categorization. “Other” category was added to survey to verify the relevance of proposed categorization, as the respondents could indicate their primary business type if not on the list. Furthermore, the question was posed the way that respondent was only able to pick one answer (the primary business sector).

According the answers, most respondents considered themselves as complete solution providers (13 respondents / 40 %). Equipment supply was chosen as primary business by seven respondents or 21 % of all respondents. Four respondents (12 %) considered themselves as tag suppliers or software/ICT suppliers, respectively. Three consulting/research companies responded the survey. Complete overview of respondents’ RFID business areas is illustrated in Figure 4.

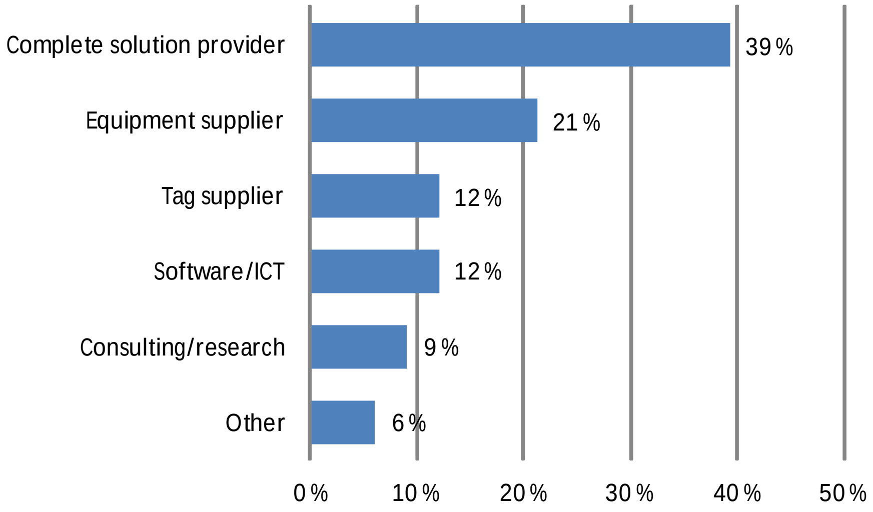


Figure 4 Survey respondents based on primary RFID business area (n=33)

In category “other”, there were two companies indicating their primary RFID business as “card manufacturing” and “pallet manufacturing” respectively. Without taking a stand on the business concept of these companies, they could probably be categorized to some other categories as well. Thus, it seems evident that the categorization created by the research team covered business areas in RFID sector and could be applied to classification.

Also the income (turnover) distribution of companies from different geographical areas was explored. Seven markets were identified: Asia, Finland, other Europe, Middle East, North-America, Russia, and South/Central America. The results are illustrated in Figure 5.

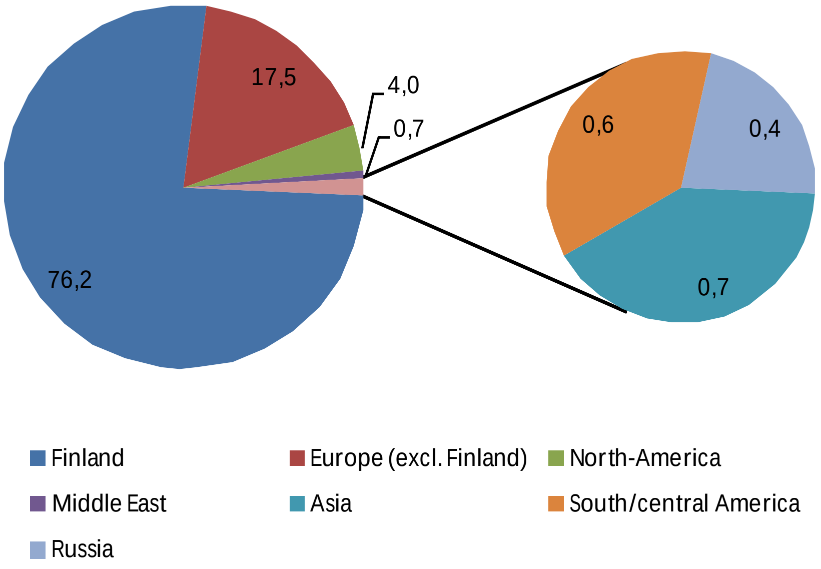


Figure 5 Geographical distribution of Finnish RFID sector based on turnover (n=33)

In average, three quarters (76.2 %) of turnover of Finnish RFID sector is generated by domestic markets. Second largest markets were other European countries with average share of 17.5 %. North-America was third biggest market with share of 4.0 %. Share of

Middle East and Asia were 0.7 % respectively, followed South/Central America 0.6 % and finally Russia with 0.4 %. It seems that Finnish RFID companies have chosen very typical way of internationalization by first penetrating to western markets. What was surprisingly thought is relatively small share of Russian markets.

3.2 Users of RFID deployments

In order to depict the current users of RFID deployments, two questions were added to survey. First of these aimed to distinguish different customer sectors, while second one mapped customers in different industries.

Three major customer sectors were identified: business-to-business (B2B), business-to-administration (B2A), and business-to-customer (B2C) sectors. Companies were asked to indicate the share of turnover generated by each sector. The results are illustrated in Figure 6.

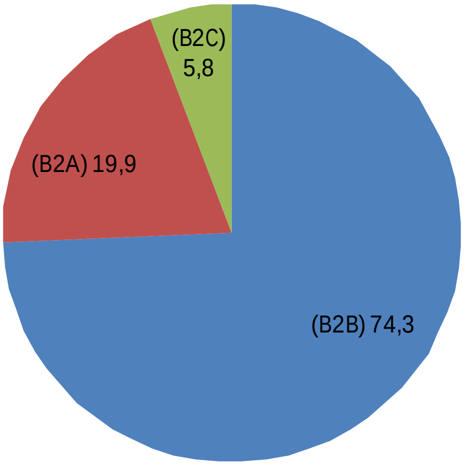


Figure 6 Share of turnover per customer sectors (n=33)

In average almost 75 % of turnover was generated by B2B sector. As it was anticipated B2A sector has second biggest contribution (around 20 %), followed by B2C sector with 5.8 % of turnover. Closer look at the results revealed that share of B2B sector accounted at least 90 % of total turnover for most of companies (17). Further, only three companies generated at least 90 % of their turnover from B2A sector. Only two companies indicated that B2A sector contributed more than 10 % of their total turnover.

Respondents were also asked to choose three most important customer sectors for their business. List followed Finnish TOL2008 industry classification and is also equivalent to international ISIC classification (Rev.4). The results are depicted with radar illustration in Figure 7.

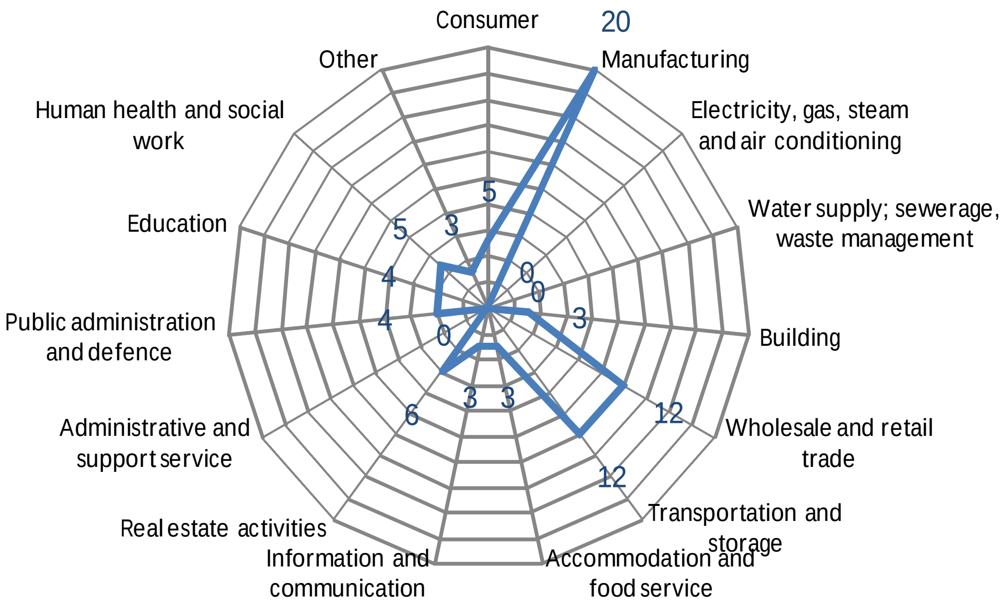


Figure 7 Most important customer segments

The main conclusion is that manufacturing (20), wholesale/retail (12), and transportation/storage (12) are three most important customer segments in general. On the other hand industries like water supply, electricity, and administrative services was not considered to be among three most important customer segments by none of the respondents. Customers segments like real estate (6), health (5), public consumer (5), administration (4), education (4), building (3), accommodation and food (3), and information and communication segment (3) were ranked among three most important segments by several companies. In category other, it was possible to respondent to identify other segments. ”Agriculture”, ”system-integrators”, and ”libraries” were identified.

Finally, the three most important customer segments are reflected to primary business areas of respondents. The main aspects aroused from cross-tabulation were dominating role of complete service providers and equipment suppliers in manufacturing and retail customer segments. Otherwise, it seems that service provision is more or less equally divided in all customer segments. It should be noticed that Table 4 should be considered only as illustrative description and no correlative conclusions should be drawn.

Table 4 Customer segments and primary business areas of Finnish RFID companies (font sizes are only for illustrative purposes)

	Software/ ICT	Complete solution provider	Equipment supplier	Tag supplier	Consulting/ research	Other
Consumer	1	3			1	
Manufacturing	3	6	5	3	2	1
Building	1		1			1
Wholesale and retail trade	2	4	4	1	1	
Transportation and storage	2	4	2	2	2	
Accommodation and food service		1		2		
Information and communication				1	1	1
Real estate activities		3	1	1		1
Administrative and support service						
Public administration and defense	1		2		1	
Education		1	1	1	1	
Electricity, gas, steam and air conditioning						
Water supply; sewerage, waste management						
Human health and social work	2	3				
Other		2		1		

3.3 Perceived challenges

In order to find out what kind of challenges companies have perceived in their business environment, the respondents were able to choose from pre-determined choices or provide own view. Technical challenges were not considered at this point, as the purpose was to survey challenges with operational nature.

Pre-determined challenges included availability of funding, fear of ICT related security risks, lack of customer awareness, no challenges perceived, and reluctance to invest. Respondents had also possibility to identify other challenges. Multiple answers were possible. The results are illustrated in Figure 8.

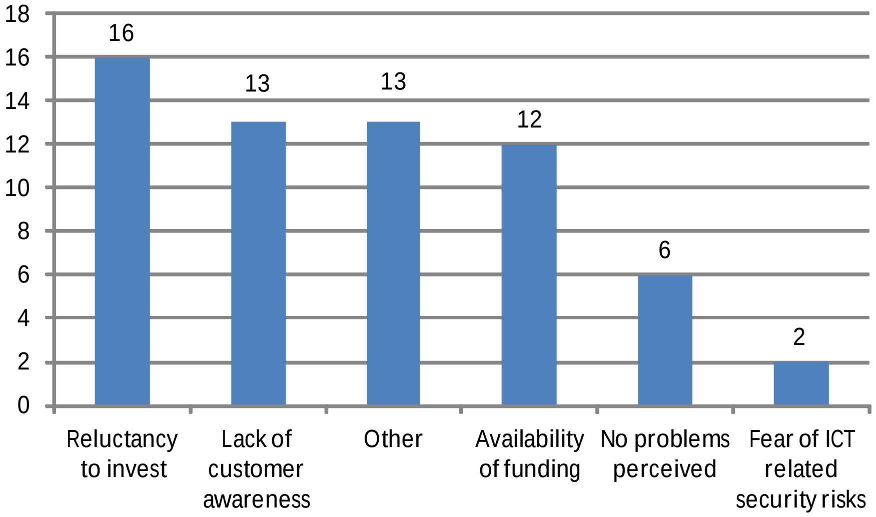


Figure 8 Perceived challenges (n=33)

As it is illustrated above, almost every other RFID company (16) identified customers' willingness to invest as a challenge. 13 companies identified the existence of lack of customer awareness. Also availability of funding was considered as challenge by several companies (12). Somewhat surprisingly, only two respondents indicated that customers' fear of ICT related security risks, poses a challenge in their business environment. Six out of 33 (18 %) RFID providers hadn't confronted any problems in their business environment.

In other category, there were 13 other challenges addressed by the respondents. Some of these were technical, but there was also interesting challenges perceived in operational environment. The challenges identified were:

- Excess bureaucracy in Finland (actions take too much time)
- The price of RFID compared to bar code
- Hinders posed by ERP-systems
- Fear of consumer opposition
- Slow penetration of NFC-phones *(identified by two respondents)*
- Inability to meet 100% reading performance
- Availability of tags (selection and delivery time)
- Monopoly of well-established actors
- Uncertain markets of RFID-phones
- Lack of public support (internalization)
- Customers' unwillingness to use integrated services
- Lack of standards

It is possible to identify some general categories of challenges. Some of these are related to technological aspects like hinders posed by ERP-systems, inability to meet 100% reading performance, and lack of standards. Others are directly related to actions of public sector like excess bureaucracy, and lack of public support for internationalization. However, the major part of other challenges is market and customer related - fear of consumer opposition, slow penetration of NFC-phones, customers' unwillingness to use integrated services, and monopoly of well-established factors. Some of these challenges can still be influenced by public sector.

4. Implementation of privacy and data protection related to RFID

The purpose of this chapter is to answer to questions concerning privacy and data protection issues related to RFID. Two main dimension surveyed were legal competence and execution of PIA.

4.1 Legal competence of RFID providers

In this subchapter, the legal competence of Finnish RFID providers is discussed. The questionnaire related to legal competence was drafted based on current legislation, which is also a foundation of PIA recommendation. This legislation was discussed in Chapter 1.2.

Two national regulations: Personal Data Act (1999/523) and Consumer Protection Act (1978/38) were included to questionnaire with three EC Directives and one recommendation:

- Directive 95/46/EC (protection of individuals with regard to the processing of personal data and on the free movement of such data)

- Directive 1999/5/EC (radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity)

- Directive 2002/58/EC (processing of personal data and the protection of privacy in the electronic communications sector)

- EC Recommendation SEC 585 2009

Questionnaire employed five-scale approach, in addition to which it was also possible for respondent to answer "not familiar" or "no answer". The results are illustrated in Figure 9.

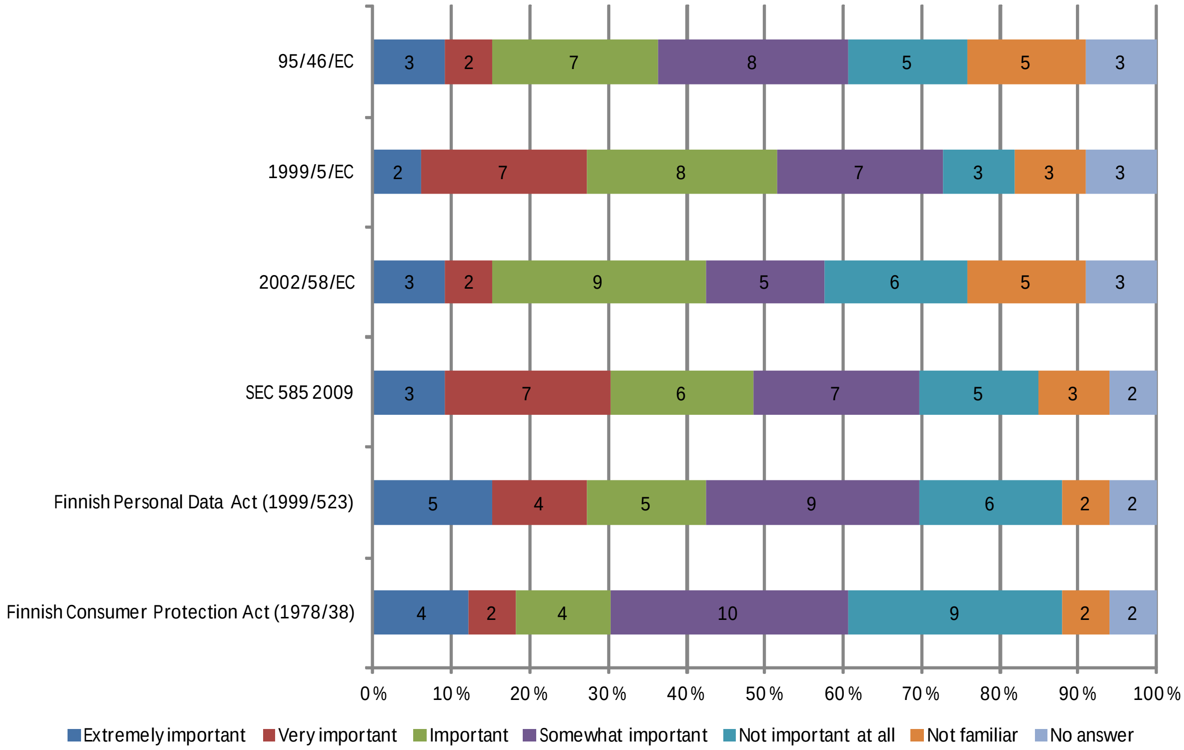


Figure 9 Legal competence of RFID providers (n=33)

According the results, over 60 % of Finnish RFID providers considered domestic legislation (1999/523 and 1978/38) at least somewhat important. Interestingly, nine respondents didn't consider consumer protection act important at all. This can be explained by the fact that according Figure 6, only five companies considered customer sector among their most important sectors. In general it seemed that based on the number of "not familiar" answers the domestic law was quite well-known.

In case of EC acts, the level of at least somewhat important acts was varying from around 58 % (2002/58/EC) to 73 % (1999/5/EC). Interestingly 30 % of respondents considered SEC 585 2009, and 28 % 1999/5/EC, as extremely or very important act. In general it can be stated that domestic acts were more often considered as extremely important as EC acts. A share of those respondents, not familiar with act at all, varied between 9-15 %, which was higher compared to Finnish acts.

The respondents were also asked to evaluate their competence in several privacy related areas including: PIA, legislation, data security and data protection. The results are illustrated in Figure 10.

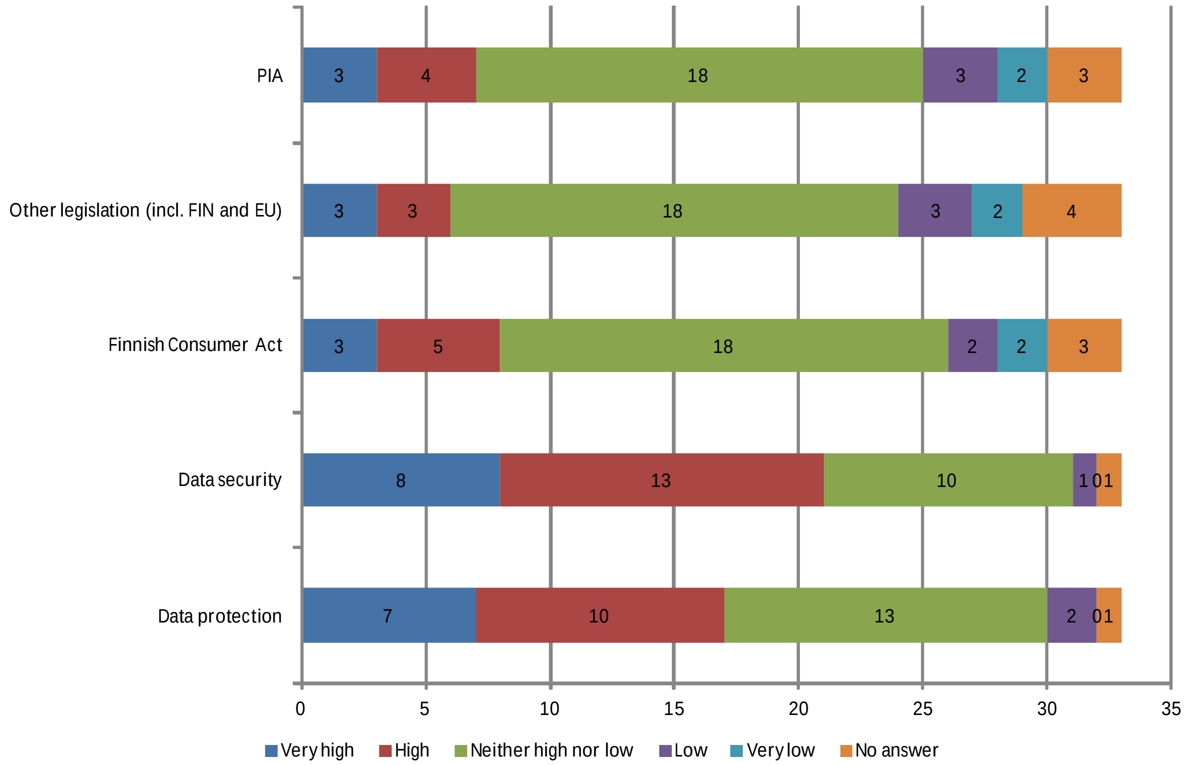


Figure 10 Competence of RFID providers (n=33)

Based on results, it seems that the competence of data security and protection issues in Finnish companies is in high level. Only one company evaluated it data security competence to be in low level. The corresponding number of companies on data protection was two. In addition none of the companies evaluated their competence in these two issues to be in very low level. Concerning the legislation and PIA issues, over half of the companies evaluated their competence to be “neither high nor low” level. Around one-third of companies evaluated their competence as high or very high. Also the number of “low” and “very low” answers was higher compared to data protection and data security. PIA is further discussed in next subchapter.

4.2 Execution of PIA

One of the goals of this survey was to study the awareness of RFID providers of PIA, and how these execute the recommendation in practice. Respondents were asked to answer the questions of PIA decision tree (see Figure 1), which output determines the need of conducting PIA and its scale. The results are illustrated in Figure 11.

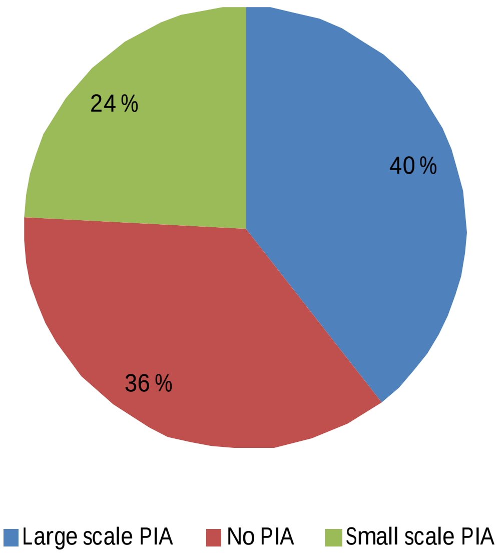


Figure 11 Need and scale of PIA among respondents (n=33)

Based on PIA decision tree questions, 40 % of respondents should conduct large scale PIA. According the answers, 24 % of respondent companies should conduct small scale PIA, while 36 % of respondents had no need of conducting PIA.

Also the knowledge of respondents concerning the PIA was surveyed. Almost one-fourth of respondents replied “no answer”, which indicates that PIA is not fully familiar for all companies. In addition, none of the 33 companies did not strongly agreed with the claims concerning their knowledge on different PIA areas. Only 2-4 companies agreed that they know PIA, which means that the rest, over 90 % of the companies, do not know PIA. These answers differ from results showed in Figure 10, according which 7 of 33 answered that their competence in PIA is high or very high.

However, it must also be remembered that not all companies need to conduct PIA. Four respondents agreed that they possess a strong knowledge on differences between small and large scale PIA, while 14 companies either disagreed or strongly disagreed. In addition, 14 companies either disagreed or strongly disagreed that they have strong knowledge on PIA risk assessment phase. The corresponding figure with initial analysis phase was 13 respondents. Nevertheless, according the results, the number of those companies that disagreed or strongly disagreed that PIA is clearly instructed by relevant authorities was somewhat smaller - nine respondents. Furthermore, 10 companies find PIA facilitating their business, while only seven disagreed or strongly disagreed. The complete distribution of answers is illustrated in Figure 12.

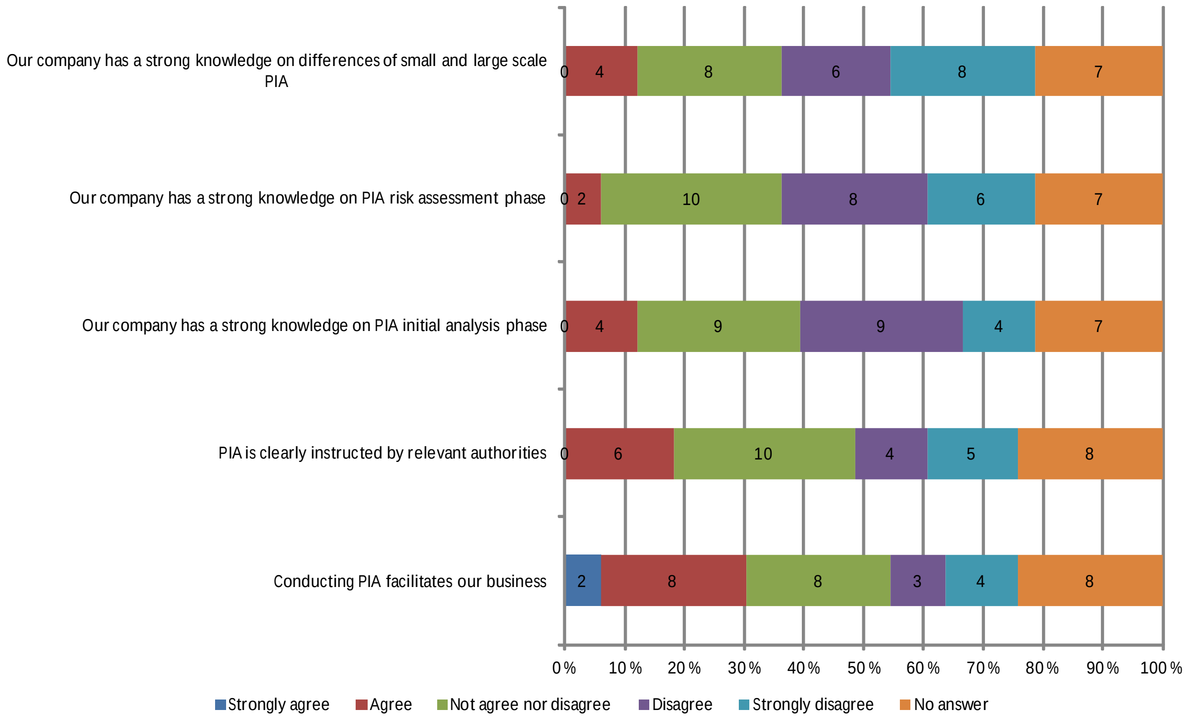


Figure 12 PIA and RFID providers (n=33)

In order to get more detailed picture of how those companies that should conduct PIA consider their knowledge, the answers were scrutinized in respect of needed scale of PIA. First, the answers concerning the knowledge on PIA is presented (Figure 13) for those companies that should not conduct PIA according their answers to PIA decision tree questions. Based on the answers, it seems quite clear that those companies that shouldn't conduct PIA didn't either consider their knowledge on framework to be important. This also explains why over 90 % of respondents either didn't answer or disagree with argument "conducting PIA facilitates our business". Also in general, the large share of blank answers can be explained the irrelevance of PIA to these companies.

Figure 14 illustrates the answers of those companies who should conduct small scale PIA. As illustrated in the figure, compared to those companies not need to conduct PIA, there was significantly less "no answers", which reflected the importance of PIA. Also, the level of "agree" answers was relatively much higher. Still, there were many companies that disagreed on the knowledge on PIA risk assessment phase. Two respondents considered their strong knowledge on initial analysis phase. According 37.5 % of those companies responsible to conduct small scale PIA, authorities have clearly instructed PIA framework, while 12.5 % disagreed and half not disagreed nor agreed.

As illustrated in Figure 15, most of companies (54 %) obligated to conduct large scale PIA strongly agreed or agreed that conducting PIA facilitates their business. Over half of respondents (54 %) also strongly agreed or agreed that PIA is clearly instructed by the relevant authorities. Finally, it can be stated that the knowledge related to conducting PIA was considered to be higher for companies obligated to large scale PIA. This indicates that those companies that are processing personal data posses also better knowledge on PIA framework.

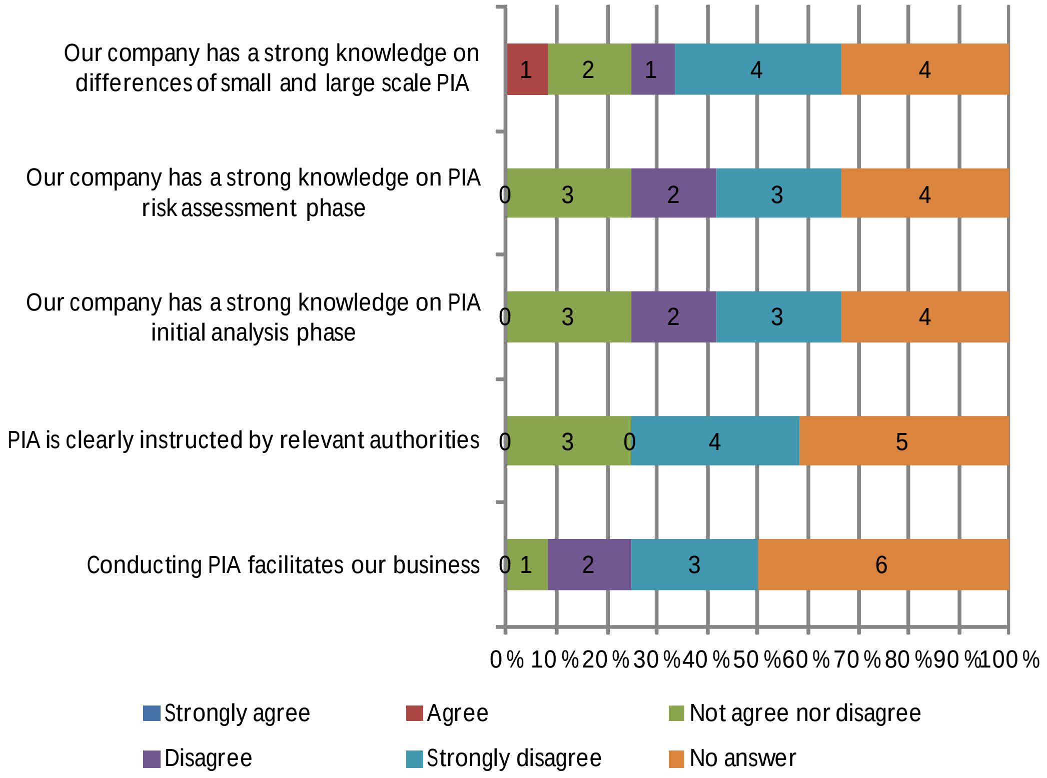


Figure 13 PIA related question for companies not needed to conduct PIA (n=12)

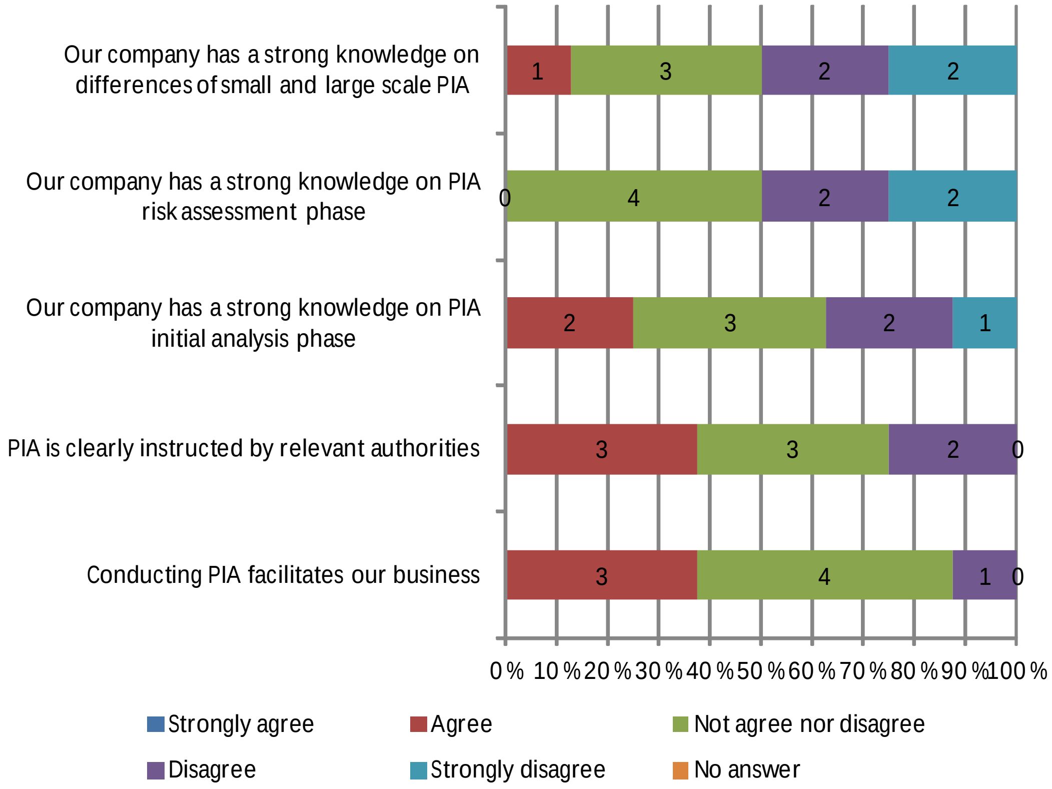


Figure 14 PIA related question for companies obligated to conduct small scale PIA (n=8)

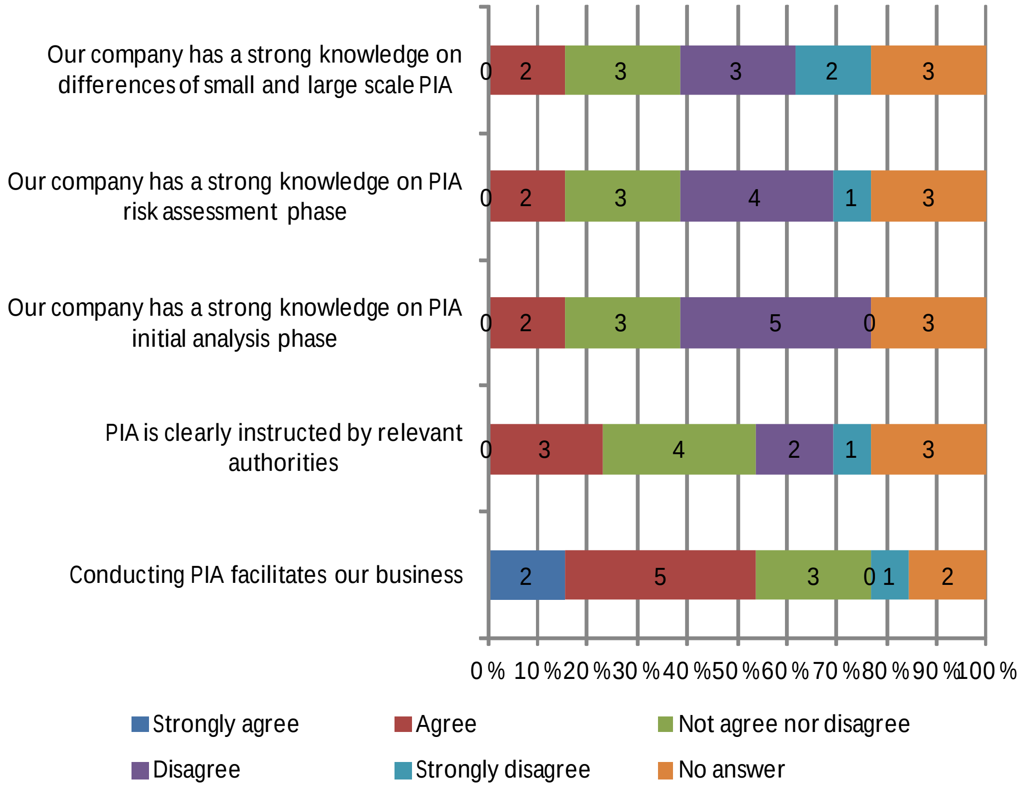


Figure 15 PIA related question for companies obligated to conduct large scale PIA (n=13)

Respondents were also asked to describe how they take PIA into consideration in practice. Few respondents indicated that they are trying to minimize the personal information in deployments in order to avoid the obligation to conduct large scale PIA. Several respondents indicated the need to conduct only a small scale PIA, but many also declared that in their business there is no need to conduct PIA at all. Few respondents also were also conducting PIA in all deployments, as the nature of their customers sectors required this. Finally, there were some respondents that indicated that they are currently exploring the impacts of PIA for their business either together with subcontractors or inside the company. In this context it was also referred to fears concerning increasing bureaucracy.

5. User requirements for usability

In final part of questionnaire it was mapped how RFID providers take usability related user requirements into consideration. Additionally, it was surveyed whether these requirements were considered to be in contradiction with data protection, privacy, or consumer act from RFID provider’s point of view. Figure 16 presents the results of the question set related to user requirements for usability.

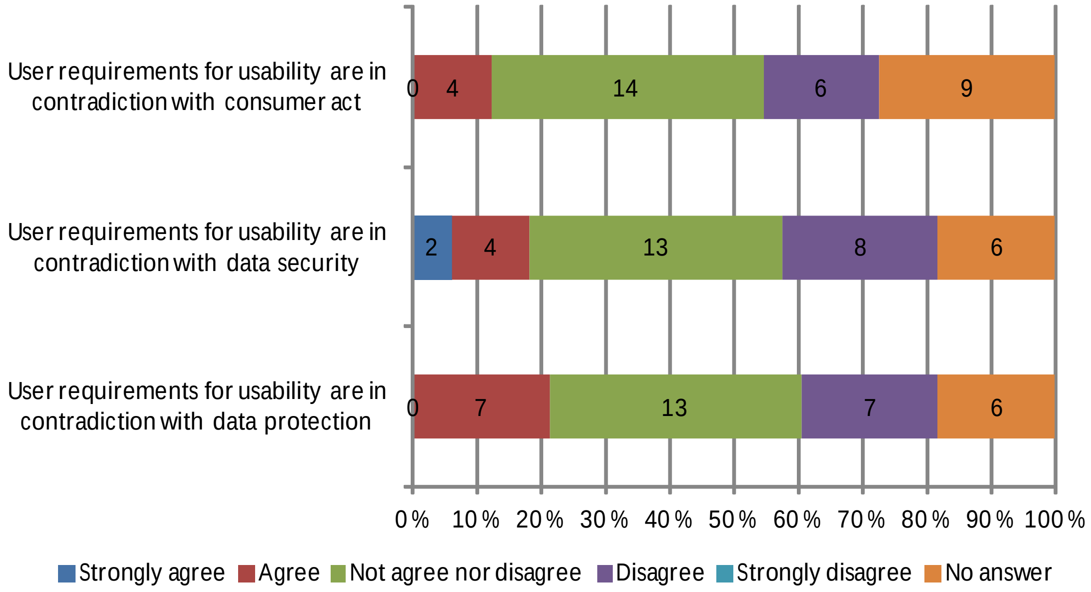


Figure 16 User requirements for usability (n=33)

There some respondent who indicated that usability requirements are in contradiction with data protection and data security, although a significant share (40 %) of respondents didn't agreed or disagreed with these arguments. Also 7 respondents disagreed. The argument according which user requirements are in some contradiction with consumer act was supported by even fewer respondents (12 %). To conclude, it seems that some contradiction had been observed, but in general there didn't seem to be major conflict.

The respondents were asked to describe how they take user requirements into consideration in practice. Especially following issues were raised by several respondents:

- Including customers to planning process, as well as close and ongoing cooperation with users covering all the details of deployment.
- Testing and usability analysis.
- Ongoing development based on customer feedback.
- Following the standards and participation of standard development

It was further asked from those respondents who identified a conflict existing, how these appear and have they taken any specific actions to mitigate the influence. Several respondents underlined the role of customer awareness and provision of enhanced data security and protection services. This also includes ICT security in general, not just RFID deployments. It was further identified, that data protection needs to be visible for customers so they can rely its reliability, but without jeopardizing the usability. Some specific issues mentioned were relationship between data protection/security and requirements of state-of-the-art innovations, role of careful planning, and user requirements related to unified credentials. Finally, the challenge of complex protection and security issues for the end users was addressed.

6. Conclusions

Due to the ability of RFID technology to operate without direct visual contact at long distances (even 6-8 meters), there is a need to privacy and data protection related legislation and recommendations in the field of RFID deployments. Furthermore, RFID infrastructure is not always easily detected by the human eye, stored information may pose a threat for consumer privacy, and passive RFID tags cannot be switched off or be put on offline mode. For these reasons, EU has published *EC Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification* (2009) and *Privacy Impact Assessment Framework for RFID applications* (2011).

RFID systems consisting of tags, readers, and databases enable several applications for both industry and consumers. Industry solutions are mainly used to improve the efficiency in supply chain or in other industrial processes (e.g. inventory solutions, identification of incoming shipments, and automated ordering). Most well-known consumer applications of RFID include access control, road tolls, payment solutions, and electronic ticketing solutions. The main benefits may include increased service quality, lower costs, improved efficiency, and added value for the customer. Especially in industrial sector, benefits are identified in improved accuracy, less throughput time, and decreased personnel. Also criticism has been presented.

Despite of its potential, RFID is still relatively marginally adopted by companies in Europe: Netherlands (9 %), Finland (8 %), Germany, Spain, Austria and Slovakia (all 4 %). The EU27 average was 3 %. The main usage was related to personnel monitoring or access control, followed by tracking and tracing solutions, payment applications, product identification, monitoring and control of production, and service/maintenance information & information/asset management. However, it has been predicted that the annual market volume of passive RFID tags in Europe will be over 86 billion in 2022 (year 2012 3.2 billion). In same year, the total number of RFID readers deployed will be over six million in Europe.

There were three main objectives in this study: 1) to depict the state of RFID sector in Finland (providers, services, customers, and challenges), 2) to survey the current stage of implementing PIA framework in Finland, and 3) to study user requirements for usability issues.

The main findings related to object one were:

- A valid classification for RFID companies is proposed to be: complete service providers, equipment suppliers, tag suppliers, software/ICT providers, consulting/research, and other.
- 39 % of respondents considered themselves as complete service providers, which indicates that one-stop-shop business model is most popular one among RFID companies.
- Over 75 % of turnover of Finnish RFID sector is generated by domestic markets. Second largest market was other European countries (17.5 %).
- Almost 75 % of turnover is generated by B2B business.
- Three most important customer segments are manufacturing, wholesale/retail, and transportation/storage.
- Almost every other respondent identified customers’ willingness to invest as a challenge. Also the lack of customer awareness and availability of funding was considered as challenge by several companies.

Several conclusions can be drawn from responses related to implementation of PIA framework:

- 60-70 % of respondents considered legislation (EU and domestic) at least somewhat important for their business.

- Competence on data security and data protection issues in Finnish companies is considered to be in high level.

- 7 out of 33 companies considered their PIA related competence to be in high or very high level.

- Based on PIA decision tree questions, 40 % of respondents may have to conduct large scale PIA, 24 % small scale PIA, and 36 % had may have no need of conducting PIA.

- Only 2-4 companies agreed that they know PIA, meaning that over 90 % of companies didn't agree to be familiar with PIA.

- Still many companies (6 of 33) agreed that PIA is clearly instructed by authorities, and facilitates their business (10 of 33).

- 28 % of those companies who may need to conduct PIA agreed that it is clearly instructed.

- 48 % of those companies who may need to conduct PIA agreed experienced it to facilitate business.

- However, it seemed that those companies that need to conduct PIA (small or large) were more familiar with the framework (interestingly there were relatively much blank answers among those companies, which need to conduct large scale PIA).

Finally, the role of user requirements for usability issues was surveyed:

- There were no major indications that user requirements were in conflict with data protection, data security of consumer act.

- The respondents took user requirements into consideration in practice by including them into the planning process, having ongoing cooperation, and by collecting customer feedback.

- Several respondents underlined the role of customer awareness and provision of enhanced data security and protection services.

Based on survey results, it seems that Finnish RFID sector is in evolving phase in many ways. The role of PIA is already identified by several actors. If the RFID takes of the way it has been predicted and the number of developments boom, also data protection and privacy related issues will probably emerge as well.

7. References

ABB's Press Release (2005) *ABB pioneers use of radio frequency identification technology in material logistics in Finland*, 4 April 2005.

Bendavid, Y. and Cassivi, L. (2010) Bridging the gap between RFID/EPC concepts, technological requirements and supply chain e-business processes. *Journal of Theoretical and Applied Electronic Commerce Research, 5*(3), 1–16.

CERP (2008) *Research Needs and Future Trends: Research in the scope of RFID and Internet of Things*, August 2008, available at <http://www.iot-visitthefuture.eu/fileadmin/documents/researchforeurope/CERP.pdf>

Directive 95/46/EC (1995) *The protection of individuals with regard to the processing of personal data and on the free movement of such data*, available at <http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm>

Directive 1999/5/EC (1999) *Radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity*, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0005:en:NOT>

Directive 2002/58/EC (2002) *Data protection in the electronic communications sector*, available at <http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm>

EC Recommendation SEC 585 (2009) *EC Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification*, 12 May 2009, available at <http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf>

EC WP 105 (2005) *Working document on data protection issues related to RFID technology*, 19 January 2005, available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf>

Eurostat News Release 12/2010 (2010), January 2010, available at <http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-19012010-BP/EN/4-19012010-BP-EN.PDF>

European passive RFID Market Sizing 2007-2022 (2007), February 2007, available at <http://www.bridge-project.eu/data/File/BRIDGE%20WP13%20European%20 passive%20RFID%20Market%20Sizing%202007-2022.pdf>

Finland commentary 00327/11/FI (2011) available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_fi.pdf>

Finkenzeller, K. (2003) *RFID Handbook - Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd Ed., John Wiley & Sons, West Sussex, England.

Frost & Sullivan (2011), *Global RFID Market*, Market Analysis, February 2011.

Granqvist, J., Permala, A and Scholliers, J. (2007) *RFTUNLOG: RFID-identification in logistics*. Espoo, Finland: VTT Technical Research Centre of Finland.

Hirsjärvi, S., Remes, P. and Sajavaara, P. (2003) *Tutki ja kirjoita*. Helsinki, Finland

Heikkilä, T. (2005) *Tilastollinen tutkimus.* Helsinki, Finland

Hobbs, G. & Streeting, M. (2009) *Fare policy reform in the smart card era,* Transportation Research Board.

Kapoor, G., Zhou, W. and Piramuthu, S. (2009) Challenges associated with RFID tag implementations in supply chains. *European Journal of Information Systems, 18*(6), 526–533.

Kotzab, H., Seuring, S., Müller, M., Reiner, G. (2005) *Research Methodologies in Supply Chain Management*. Heidelberg, Germany

Kärkkäinen, M. (2003) Increasing efficiency in the supply chain for short shelf life goods using RFID tagging. *International Journal of Retail & Distribution Management, 31*(10), 529–536.

McFarlane, D. and Sheffi, Y. (2003) The impact of automatic identification on supply chain operations. *The International Journal of Logistics Management, 14*(1), 1–17.

McNeill, P. and Chapman, S. (2005) *Research methods,* 3rd Edition, Oxon, England.

Murto, L. - Sipola, M. (2010) *RFID/NFC -Tekniikan vaikutus kuluttajiin.* Turun AMK/Tietojenkäsittely, opinnäytetyö, Turku, Finland.

Naula, T., Ojala, L., Solakivi, T., Takalokastari, M., Rantanen, M., Kalske, M., Engblom, J., Häkkinen, L., Essén, T., Töyli, J. and Stenholm, P. (2006) *Finland's state of logistics survey 2006*. Publications of the Ministry of Transport and Communications, 2006(35).

NP company overview, available at <http://www.np-collection.com/index.php?option=com_content&view=article&id=52&Itemid=76&lang=en>

NP Smart Clothing Store, available at <http://www.np-collection.com/index.php?option=com_content&view=article&id=75&Itemid=50&lang=en>

Permala, A., Scholliers, J., and Granqvist, J. (2006) *RFID-roadmap for business logistics*. Liikenne- ja viestintäministeriö AINO-julkaisuja: 30, Helsinki.

Permala, A., Scholliers, J. and Granqvist, J. (2006) *Logistiikan RFID - Teknologiakatsaus*. Liite raporttiin Etätunnistuksen suuntaviivat logistiikassa. Liikenne- ja viestintäministeriö AINO-julkaisuja: 30B, Helsinki.

Permala, A., Pilli-Sihvola, E., Rantasila, K. and Scholliers, J. (2011) *RFID–A Supporting Technology for Paperless Logistics*, paper presented at the e-Freight Conference, Münich, 10–11 May 2011.

Permala, A. and Scholliers, J. (2008) *Demonstration of the Use of Passive RFID in Logistics services in Finland*, paper presented at 15th World Congress on Intelligent Transport Systems, 16–20 Nov. 2008, New York.

PIA Framework for RFID Applications (2011), available at <http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf>

PIAw@tch - the Privacy Impact Assessment observatory, Finland. Available at <http://www.piawatch.eu/node/207>

Privacy International, Finland. Available at <https://www.privacyinternational.org/survey/phr2003/countries/finland.htm>

Pilli-Sihvola, E., Rantasila, K. and Permala, A. (2011) *RFID, a promise of improved visibility in the supply chain*. NOFOMA Conference, June 9-10, 2011, Proceedings. Dep. of Business Administration and Social Sciences. Harstad, Norway (2011), Paper 45419

RFID Lab Finland, available at <http://www.rfidlab.fi/eng/rfid-lab-finland>

RFID Lab Finland Case Bank/Case ABB, available at <http://www.rfidlab.fi/sites/rfidlab.fi/files/ABB_outbound_RFID_press_FI_090417.pdf>

RFID Lab Finland/Case NP, available at: <http://www.rfidlab.fi/sites/rfidlab.fi/files/Naisten%20Pukutehdas_0_0.pdf>

Rida, A., Li, Y., Tentzeris, M.M. and Mortazawi, A. (2009) Design and Development of RFID and RFID-enabled sensors on flexible low cost substrates. *Synthesis Lectures on RF/Microwaves, 1*(1), 1–89.

Swedberg, C. (2008) *Clothing Designer Brings RFID to Its Shoppers*, RFID Journal, 5 December, available at <http://www.rfidjournal.com/article/view/4485/1/1/>

Tancock, D. - Pearson, S. and Charlesworth, A. (2010) *The Emergence of Privacy Impact Assessments*. HPL-2010-63, available at <http://www.hpl.hp.com/techreports/2010/HPL-2010-63.pdf>

The Charter of Fundamental Rights of the European Union (2000) available at: <http://www.europarl.europa.eu/charter/default_en.htm>

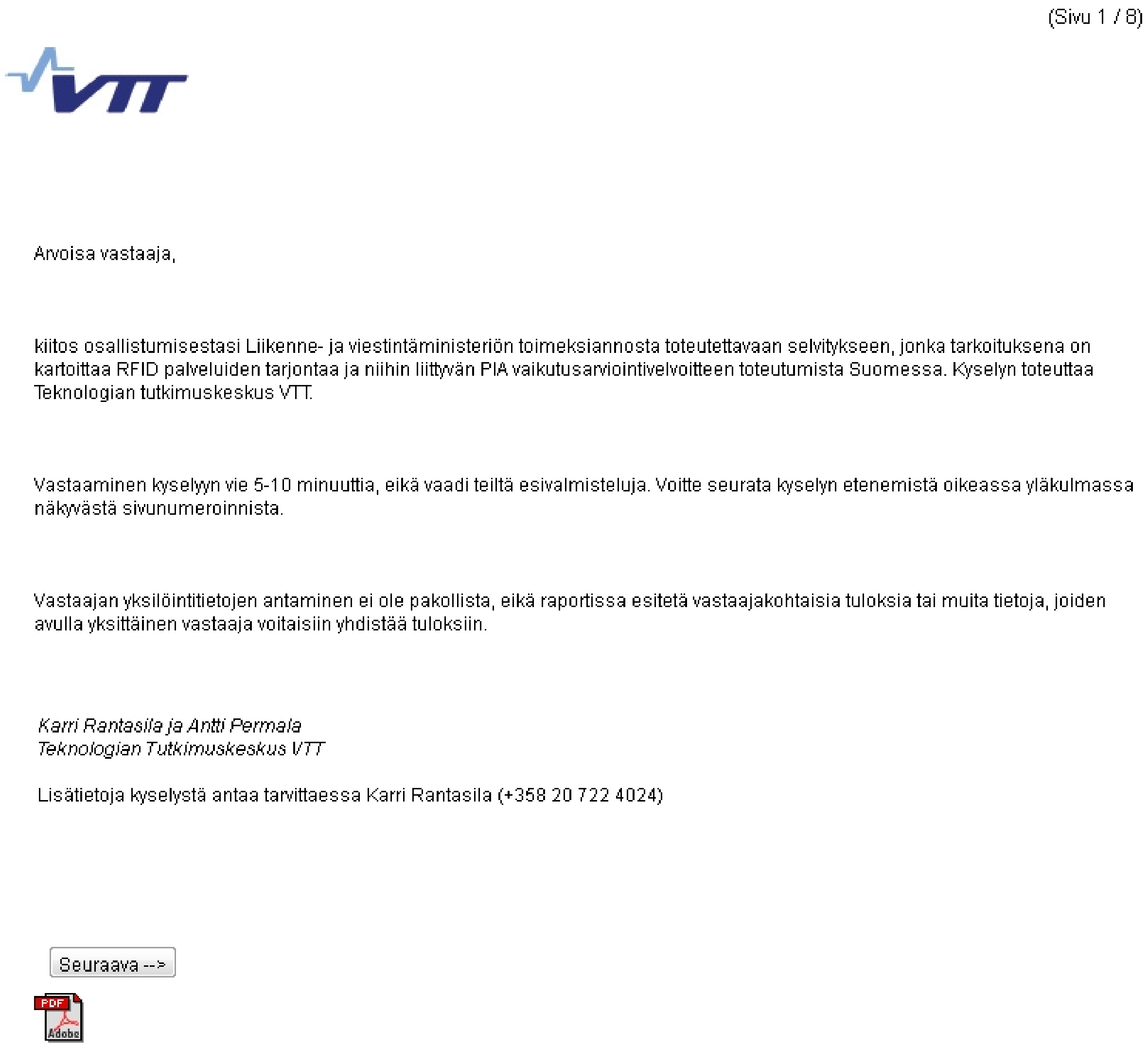
UITP Position Paper (2007) *Everybody Local Everywhere*, UITP Position Paper.

Wessel, R. (2009) *RFID Drives Up Efficiencies at ABB*, RFID Journal, 25 November 2009.

Wimmer, T. and Nathanson, D. (2010) *Barcode and RFID Market Update & 2010 Outlook*, webcast presentation January 20th 2010

Zuo, Y. (2010) Survivable RFID Systems: Issues, challenges, and techniques. *IEEE Transactions on Systems, Man & Cybernetics: Part C – Applications & Reviews*, *40*(4), 406–418.

8. Annex: Question set



(Sivu 1 / 8)

Arvoisa vastaaja,

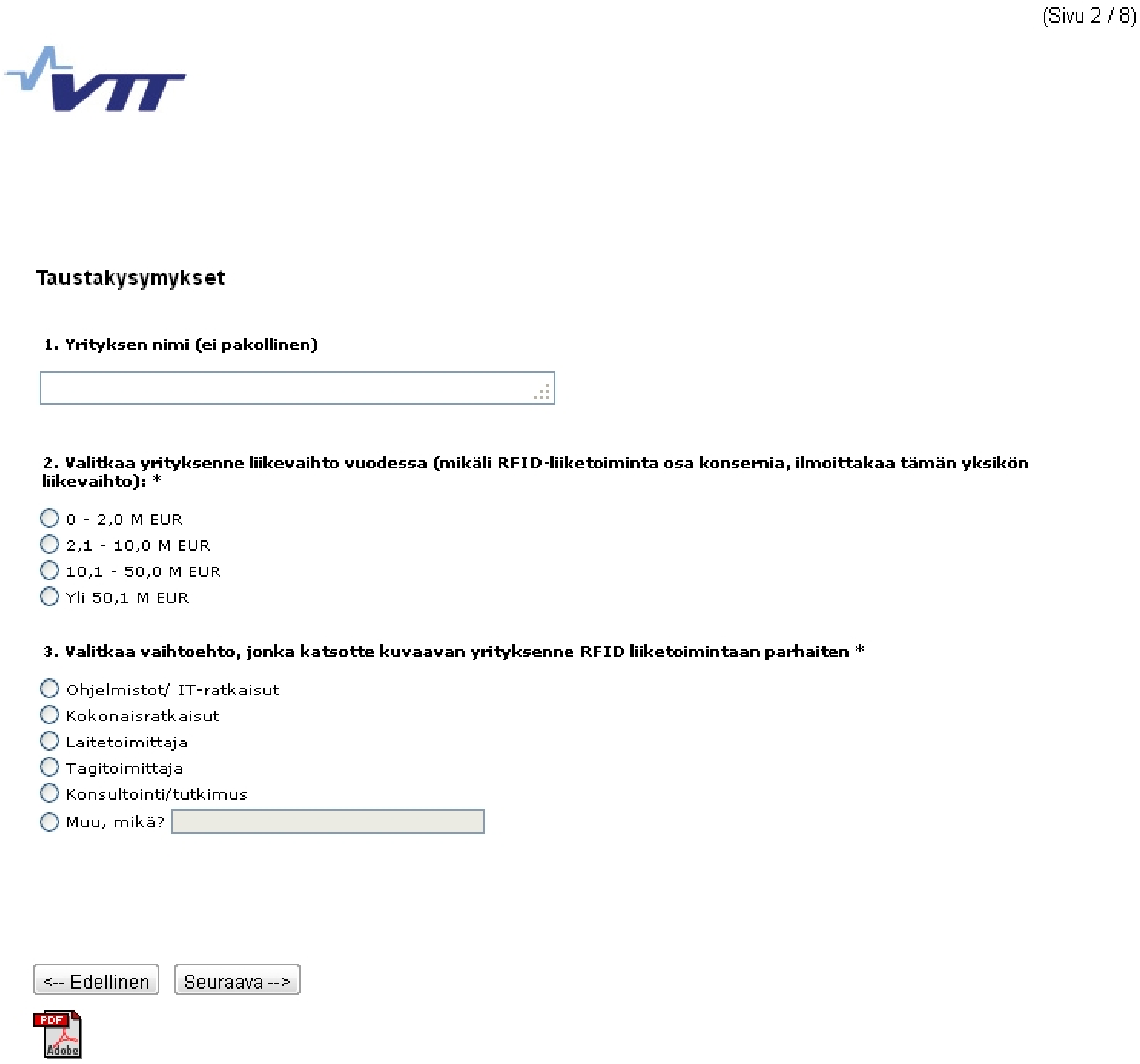
kiitos osallistumisestasi Liikenne- ja viestintäministeriön toimeksiannosta toteutettavaan selvitykseen, jonka tarkoituksena on kartoittaa RFID palveluiden tarjontaa ja niihin liittyvän PIA vaikutusarviointivelvoitteen toteutumista Suomessa. Kyselyn toteuttaa Teknologian tutkimuskeskus VTT.

Vastaaminen kyselyyn vie 5-10 minuuttia, eikä vaadi teiltä esivalmisteluja. Voitte seurata kyselyn etenemistä oikeassa yläkulmassa näkyvästä sivunumeroinnista.

Vastaajan yksilöintitietojen antaminen ei ole pakollista, eikä raportissa esitetä vastaajakohtaisia tuloksia tai muita tietoja, joiden avulla yksittäinen vastaaja voitaisiin yhdistää tuloksiin.

Karri Rantasila ja Antti Permala
Teknologian Tutkimuskeskus VTT

Lisätietoja kyselystä antaa tarvittaessa Karri Rantasila (+358 20 722 4024)



(Sivu 2 / 8)

Taustakysymykset

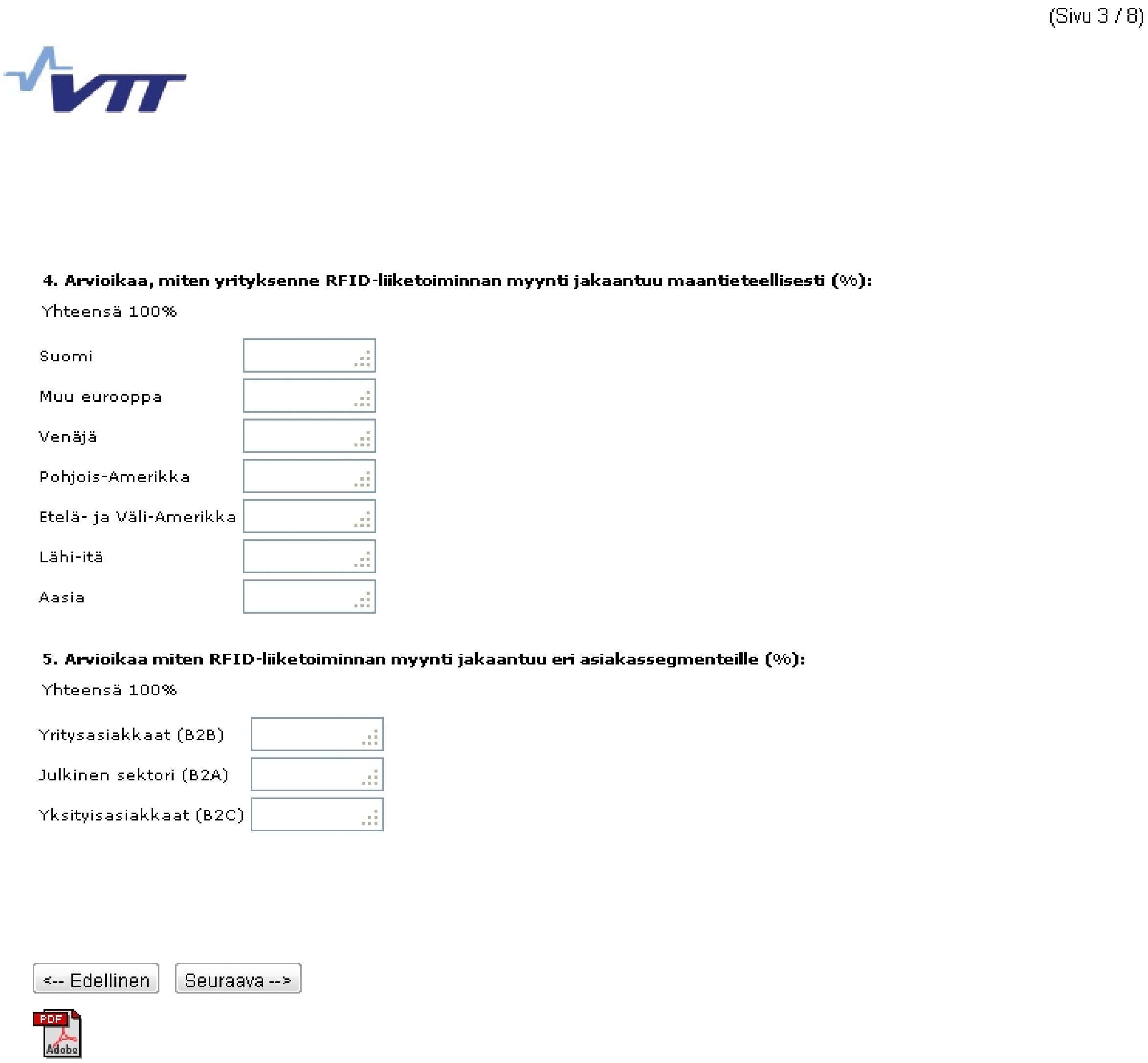
1. Yrityksen nimi (ei pakollinen)

2. Valitkaa yrityksenne liikevaihto vuodessa (mikäli RFID-liiketoiminta osa konsernia, ilmoittakaa tämän yksikön liikevaihto): *

○ 0 - 2,0 M EUR
○ 2,1 - 10,0 M EUR
○ 10,1 - 50,0 M EUR
○ Yli 50,1 M EUR

3. Valitkaa vaihtoehto, jonka katsotte kuvaavan yrityksenne RFID liiketoimintaan parhaiten *

○ Ohjelmistot/ IT-ratkaisut
○ Kokonaisratkaisut
○ Laitetoimittaja
○ Tagitoimittaja
○ Konsultointi/tutkimus
○ Muu, mikä?



(Sivu 3 / 8)

4. Arvioikaa, miten yrityksenne RFID-liiketoiminnan myynti jakaantuu maantieteellisesti (%):

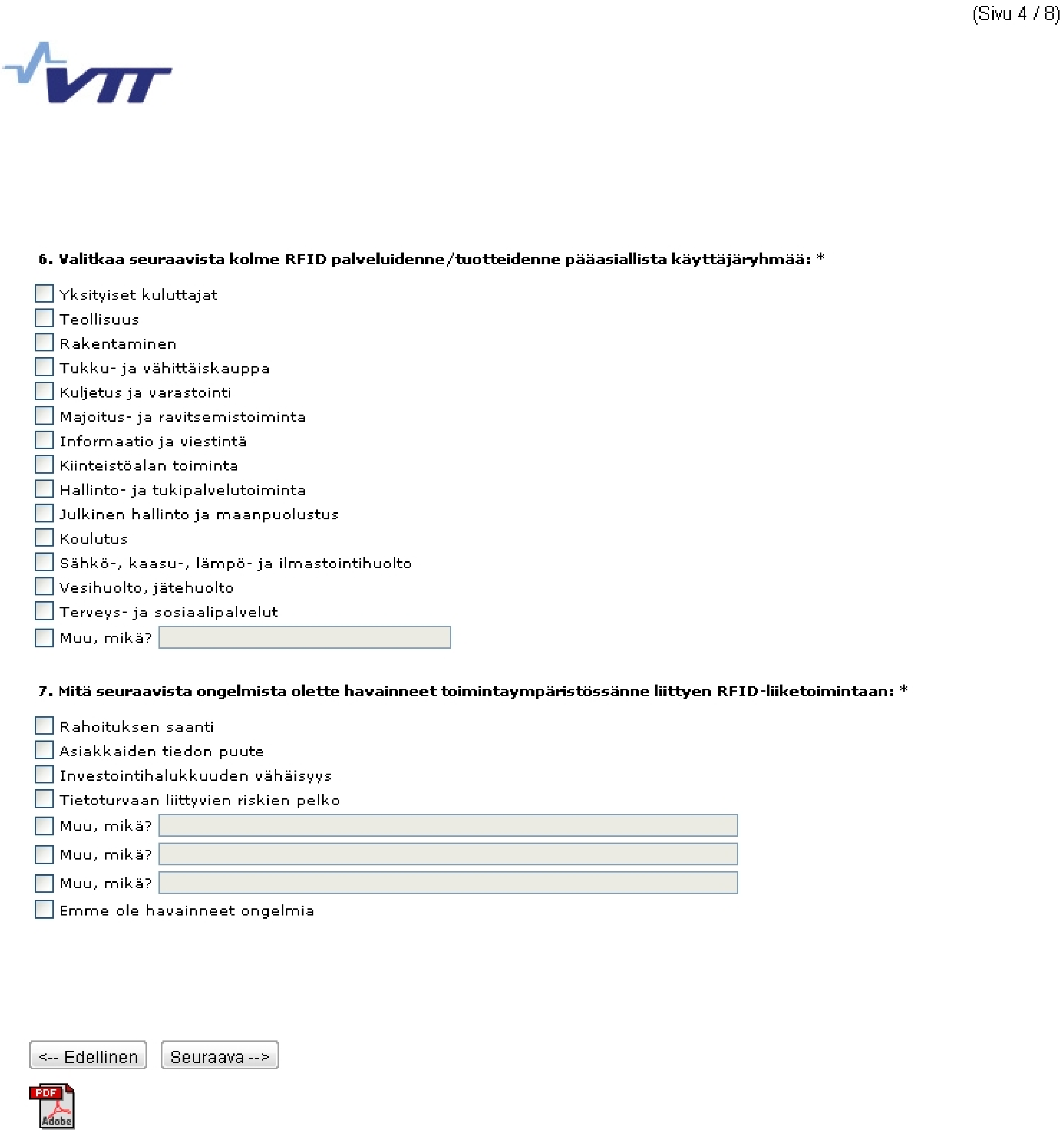
Yhteensä 100%

Suomi	
Muu eurooppa	
Venäjä	
Pohjois-Amerikka	
Etelä- ja Väli-Amerikka	
Lähi-itä	
Aasia	

5. Arvioikaa miten RFID-liiketoiminnan myynti jakaantuu eri asiakassegmenteille (%):

Yhteensä 100%

Yritysasiakkaat (B2B)	
Julkinen sektori (B2A)	
Yksityisasiakkaat (B2C)	



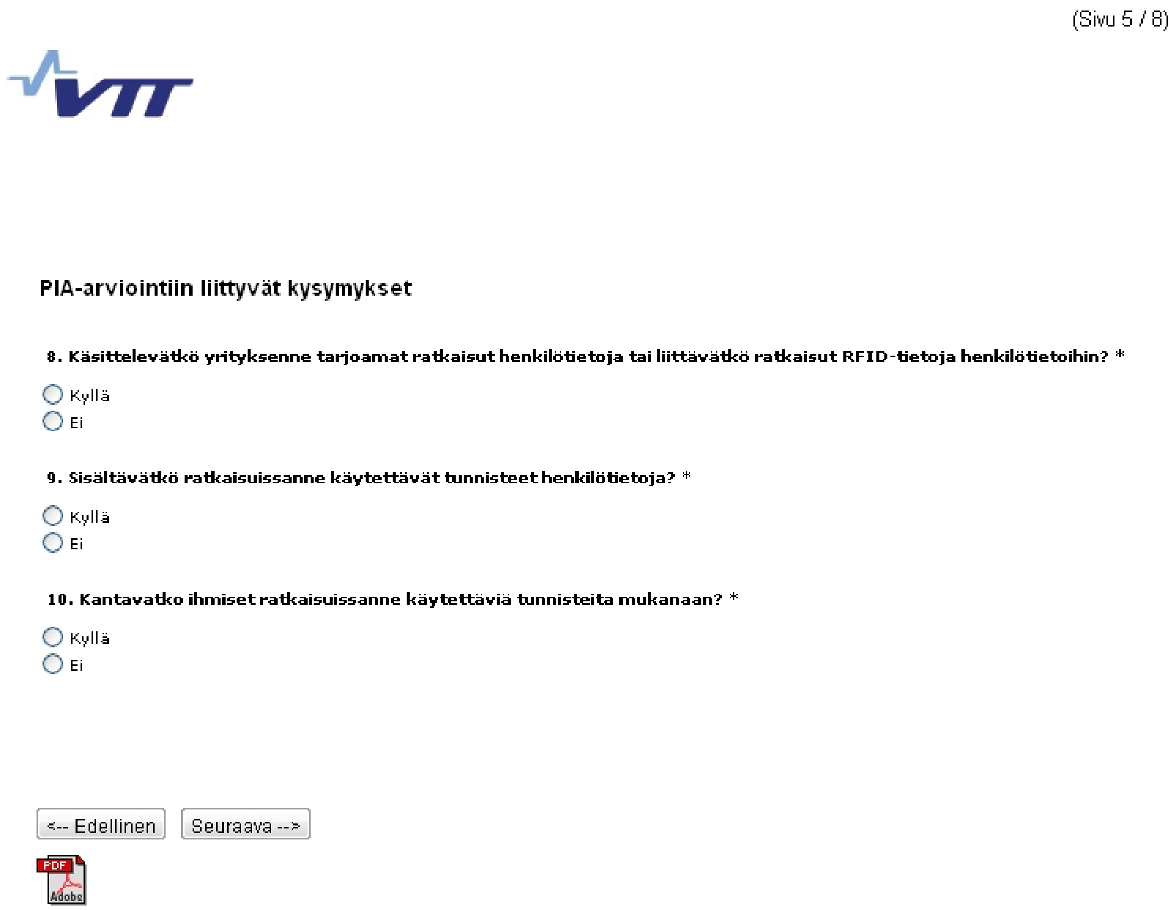
(Sivu 4 / 8)

6. Valitkaa seuraavista kolme RFID palveluidenne/tuotteidenne pääasiallista käyttäjäryhmää: *

□ Yksityiset kuluttajat
□ Teollisuus
□ Rakentaminen
□ Tukku- ja vähittäiskauppa
□ Kuljetus ja varastointi
□ Majoitus- ja ravitsemistoiminta
□ Informaatio ja viestintä
□ Kiinteistöalan toiminta
□ Hallinto- ja tukipalvelutoiminta
□ Julkinen hallinto ja maanpuolustus
□ Koulutus
□ Sähkö-, kaasu-, lämpö- ja ilmastointihuolto
□ Vesihuolto, jätehuolto
□ Terveys- ja sosiaalipalvelut
□ Muu, mikä?

7. Mitä seuraavista ongelmista olette havainneet toimintaympäristössänne liittyen RFID-liiketoimintaan: *

□ Rahoituksen saanti
□ Asiakkaiden tiedon puute
□ Investointihalukkuuden vähäisyys
□ Tietoturvaan liittyvien riskien pelko
□ Muu, mikä?
□ Muu, mikä?
□ Muu, mikä?
□ Emme ole havainneet ongelmia



(Sivu 5 / 8)

PIA-arviointiin liittyvät kysymykset

8. Käsittelevätkö yrityksenne tarjoamat ratkaisut henkilötietoja tai liittävätkö ratkaisut RFID-tietoja henkilötietoihin? *

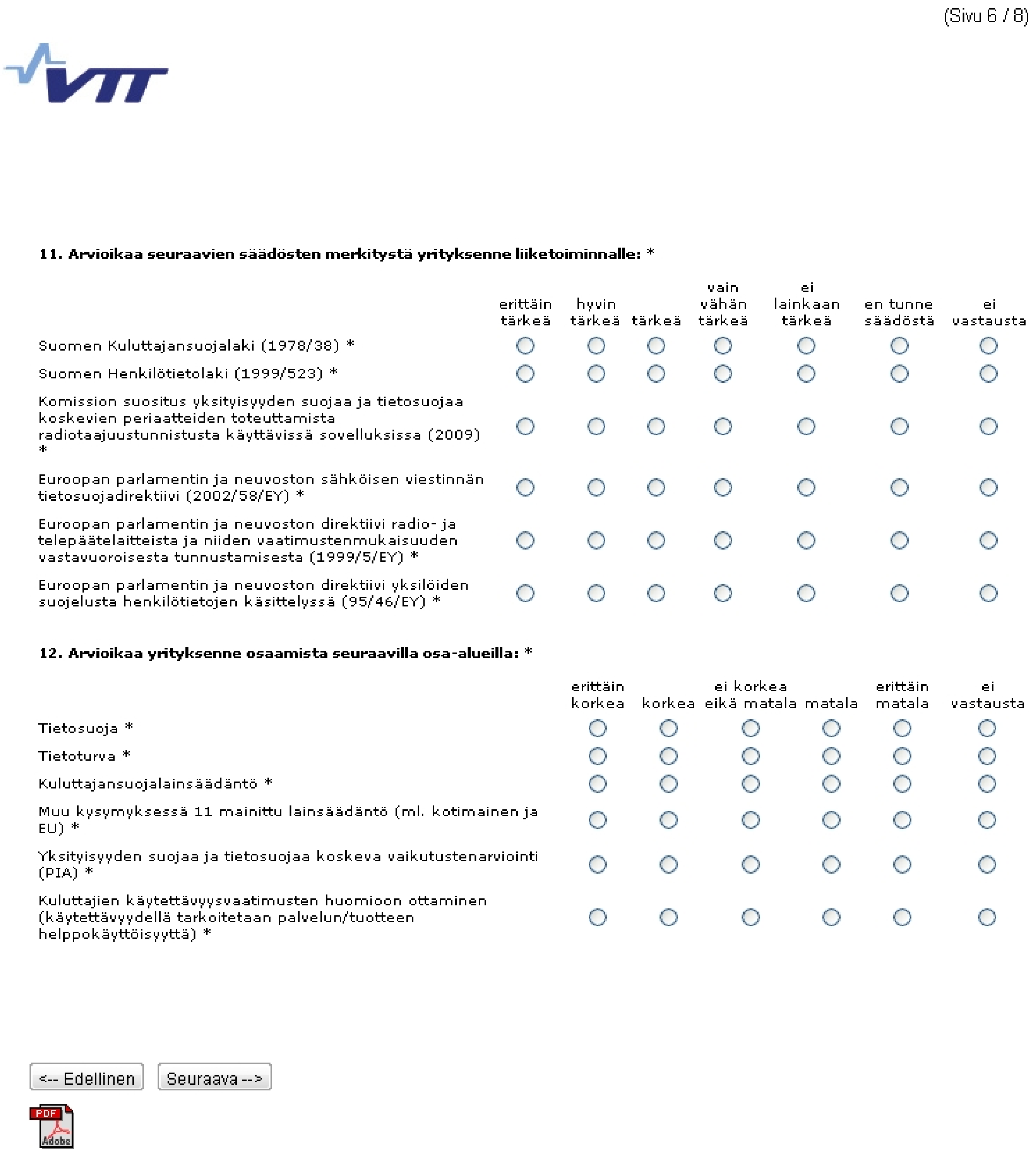
○ Kyllä
○ Ei

9. Sisältävätkö ratkaisuissanne käytettävät tunnisteet henkilötietoja? *

○ Kyllä
○ Ei

10. Kantavatko ihmiset ratkaisuissanne käytettäviä tunnisteita mukanaan? *

○ Kyllä
○ Ei



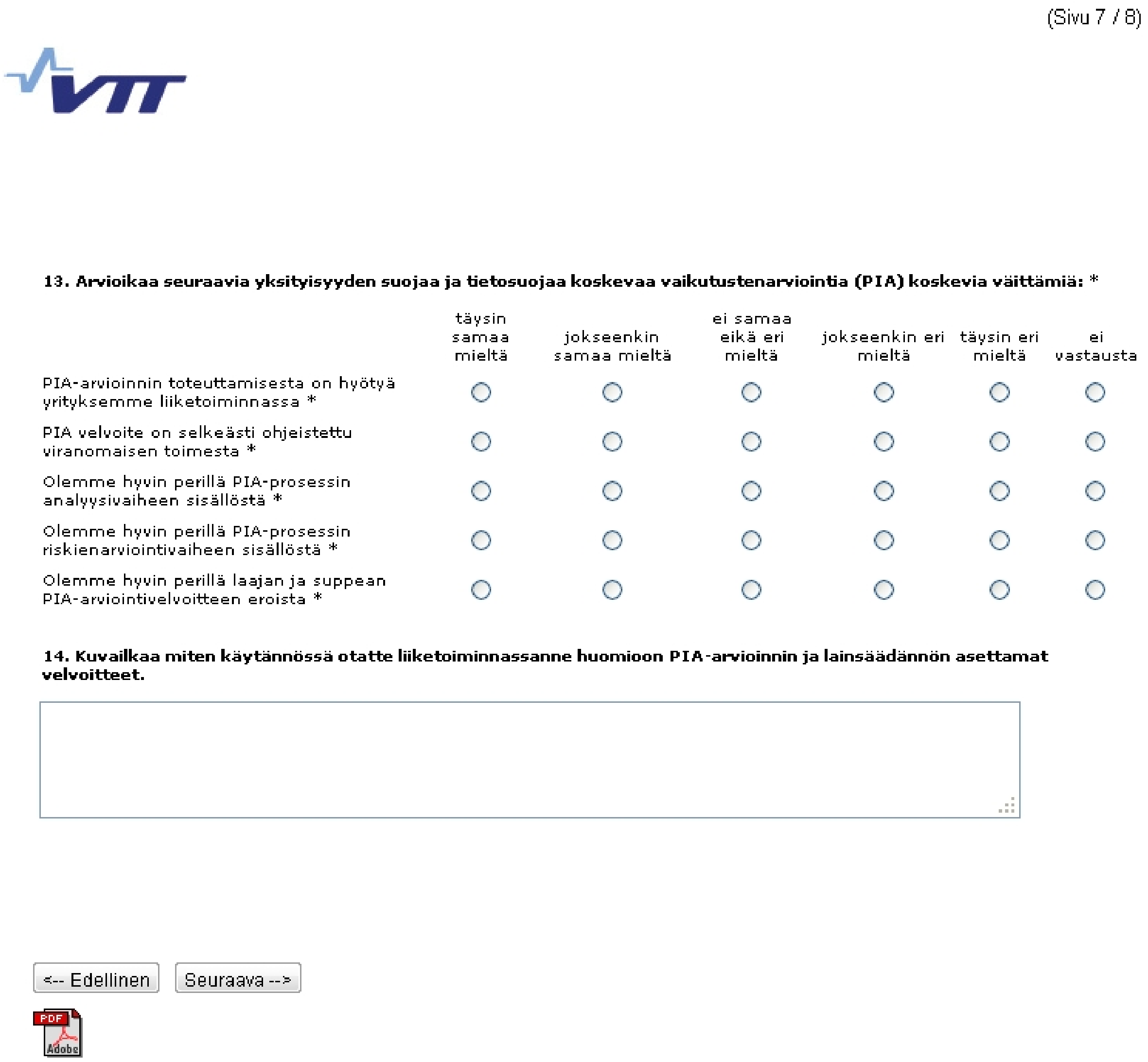
(Sivu 6 / 8)

11. Arvioikaa seuraavien säädösten merkitystä yrityksenne liiketoiminnalle: *

	erittäin tärkeä	hyvin tärkeä	tärkeä	vain vähän tärkeä	ei lainkaan tärkeä	en tunne säädöstä	ei vastausta
Suomen Kuluttajansuojalaki (1978/38) *	○	○	○	○	○	○	○
Suomen Henkilötietolaki (1999/523) *	○	○	○	○	○	○	○
Komission suositus yksityisyyden suojaa ja tietosuojaa koskevien periaatteiden toteuttamista radiotaajuustunnistusta käyttävissä sovelluksissa (2009) *	○	○	○	○	○	○	○
Euroopan parlamentin ja neuvoston sähköisen viestinnän tietosuojadirektiivi (2002/58/EY) *	○	○	○	○	○	○	○
Euroopan parlamentin ja neuvoston direktiivi radio- ja telepäätelaitteista ja niiden vaatimustenmukaisuuden vastavuoroisesta tunnustamisesta (1999/5/EY) *	○	○	○	○	○	○	○
Euroopan parlamentin ja neuvoston direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä (95/46/EY) *	○	○	○	○	○	○	○

12. Arvioikaa yrityksenne osaamista seuraavilla osa-alueilla: *

	erittäin korkea	korkea	ei korkea eikä matala	matala	erittäin matala	ei vastausta
Tietosuoja *	○	○	○	○	○	○
Tietoturva *	○	○	○	○	○	○
Kuluttajansuojalainsäädäntö *	○	○	○	○	○	○
Muu kysymyksessä 11 mainittu lainsäädäntö (ml. kotimainen ja EU) *	○	○	○	○	○	○
Yksityisyyden suojaa ja tietosuojaa koskeva vaikutustenarviointi (PIA) *	○	○	○	○	○	○
Kuluttajien käytettävyysvaatimusten huomioon ottaminen (käytettävyydellä tarkoitetaan palvelun/tuotteen helppokäyttöisyyttä) *	○	○	○	○	○	○

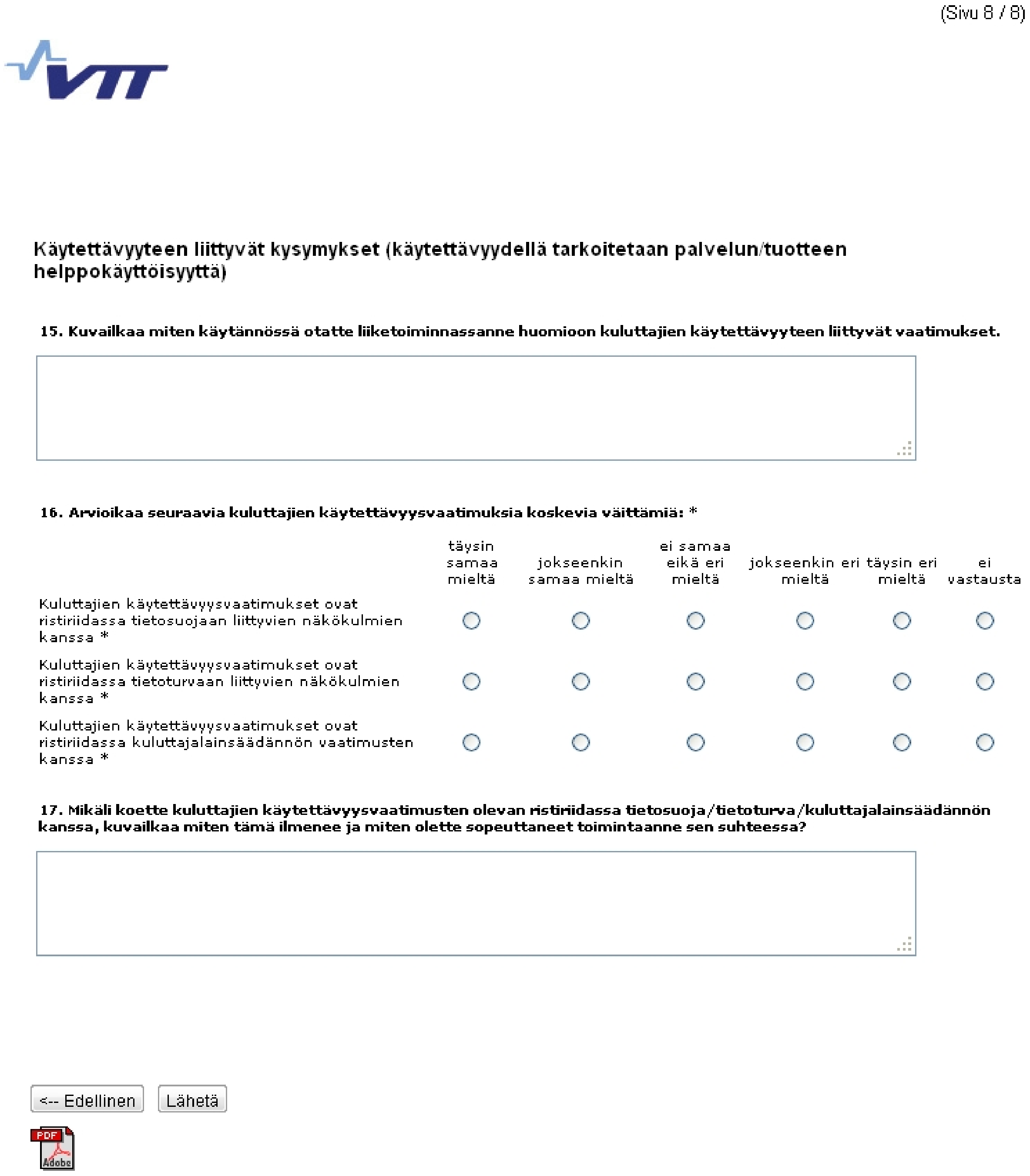


(Sivu 7 / 8)

13. Arvioikaa seuraavia yksityisyyden suojaa ja tietosuojaa koskevaa vaikutustenarviointia (PIA) koskevia väittämiä: *

	täysin samaa mieltä	jokseenkin samaa mieltä	ei samaa eikä eri mieltä	jokseenkin eri mieltä	täysin eri mieltä	ei vastausta
PIA-arvioinnin toteuttamisesta on hyötyä yrityksemme liiketoiminnassa *	○	○	○	○	○	○
PIA velvoite on selkeästi ohjeistettu viranomaisen toimesta *	○	○	○	○	○	○
Olemme hyvin perillä PIA-prosessin analyysivaiheen sisällöstä *	○	○	○	○	○	○
Olemme hyvin perillä PIA-prosessin riskienarviointivaiheen sisällöstä *	○	○	○	○	○	○
Olemme hyvin perillä laajan ja suppean PIA-arviointivelvoitteen eroista *	○	○	○	○	○	○

14. Kuvailkaa miten käytännössä otatte liiketoiminnassanne huomioon PIA-arvioinnin ja lainsäädännön asettamat velvoitteet.



(Sivu 8 / 8)

Käytettävyyteen liittyvät kysymykset (käytettävyydellä tarkoitetaan palvelun/tuotteen helppokäyttöisyyttä)

15. Kuvailkaa miten käytännössä otatte liiketoiminnassanne huomioon kuluttajien käytettävyyteen liittyvät vaatimukset.

16. Arvioikaa seuraavia kuluttajien käytettävyysvaatimuksia koskevia väittämiä: *

	täysin samaa mieltä	jokseenkin samaa mieltä	ei samaa eikä eri mieltä	jokseenkin eri mieltä	täysin eri mieltä	ei vastausta
Kuluttajien käytettävyysvaatimukset ovat ristiriidassa tietosuojaan liittyvien näkökulmien kanssa *	○	○	○	○	○	○
Kuluttajien käytettävyysvaatimukset ovat ristiriidassa tietoturvaan liittyvien näkökulmien kanssa *	○	○	○	○	○	○
Kuluttajien käytettävyysvaatimukset ovat ristiriidassa kuluttajalainsäädännön vaatimusten kanssa *	○	○	○	○	○	○

17. Mikäli koette kuluttajien käytettävyysvaatimusten olevan ristiriidassa tietosuoja/tietoturva/kuluttajalainsäädännön kanssa, kuvailkaa miten tämä ilmenee ja miten olette sopeuttaneet toimintaanne sen suhteessa?