Building **R**adio frequency **ID**entification for the **G**lobal **E**nvironment

Security Analysis Report

Authors: BT Research, ETH Zurich, Technical University Graz,SAP Research, AT4 wireless, Benedicta, Universitat de Catalunya, Caen, Confidex,Fudan University, UPM Rafalatac, GS1 UK.

11 July 2007

This work has been partly funded by the European Commission contract No: IST-2005-033546

About the BRIDGE Project:

BRIDGE (**B**uilding **R**adio frequency **ID**entification for the **G**lobal **E**nvironment) is a 13 million Euro RFID project running over 3 years and partly funded (€7,5 million) by the European Union. The objective of the BRIDGE project is to research, develop and implement tools to enable the deployment of EPCglobal applications in Europe. Thirty interdisciplinary partners from 12 countries (Europe and Asia) are working together on : Hardware development, Serial Look-up Service, Serial-Level Supply Chain Control, Security; Anti-counterfeiting, Drug Pedigree, Supply Chain Management, Manufacturing Process, Reusable Asset Management, Products in Service, Item Level Tagging for non-food items as well as Dissemination tools, Education material and Policy recommendations.

For more information on the BRIDGE project: www.bridge-project.eu

This document:

The goal of this report is to analyze the state-of-the-art and elaborate security requirements for BRIDGE.

Disclaimer:

This document results from work being done in the framework of the BRIDGE project. It does not represent an official deliverable formally approved by the European Commission.

Authors and Contributors

Work package leader	Andrea Soppera (BT Research)
Editor of deliverable	Alexander Ilic (ETH Zürich)
Authors (alphabetical)	Manfred Aigner (TU Graz) Trevor Burbridge (BT Research) Ali Dada (SAP Research) Jeff Farr (BT Research) Alexander Ilic (ETH Zürich) Andrea Soppera (BT Research)
Contributors	Robert Maidment (GS1-UK) Mikko Lehtonen (ETH Zürich) Team Contribution (AT4Wireless)
Reviewers	Cosmin Condea (SAP Research) Annamaria Colonna (CAEN)

Acknowledgements
We would like to thank all interview partners for their time and their valuable input.

Executive Summary

The goal of this report is to analyze the state-of-the-art and elaborate security requirements for BRIDGE. BRIDGE goes beyond the specification of the traditional EPC network architecture by enhancing the network access and connectivity layer and by adding an application layer. This intended infrastructure is referred to as Extended EPC Network architecture. A security assessment of the state-of-the-art shows that the local EPC network components such as tags and readers can be deployed securely within constrained environments involving a limited number of trusted parties. Proprietary software developments combined with measures of traditional Internet security help to seal off the network, systems and data from those outside the limited group. The intention of BRIDGE is to also allow the deployment of RFID to enable dynamic cross party applications where the participants may not be known at the time of deployment, and where there are conflicting interests between such parties. For such global deployments, a strong requirement for standards and standardized interfaces emerges. The security analysis indicates that a higher level of security is needed for existing EPC Network components such as tags and readers to operate in such open environments. In addition the network to share information securely between organisations is not yet developed. Our key conclusion is that security is a multi-layered problem and the strength of any solution is dependent on the security of the weakest link.

To derive requirements for this complex problem, two sources of input were used. First, the security concerns and requirements of end-users of RFID across different industries were captured by face-to-face and telephone interviews. Second, the security experts of work package WP4 “Security” collaborated with work package WP2 “Serial-Level Lookup Service” to construct probable scenarios for more open and collaborative uses of RFID. These were analysed through use and misuse cases spanning all the components of the multi-layer architecture to determine attacks and technical security requirements. The output of this process is documented in this report and should act as a guideline for others inside and outside the BRIDGE project. Note that our approach is application and scenario-dependant, and deployments of RFID should perform further analysis within their own context.

To conclude, our goal is to remove the security barriers to new RFID applications across dynamic and collaborative supply chains. Such applications will only provide value if we can protect business intelligence and operate secure processes over data received from external parties. We have analysed the security requirements to support these applications and suggested a programme of technical work to provide the required tools to the developers of both RFID systems and international standards.

Terms and definitions

Attack: A certain way to exploit a vulnerability of the system.

Closed-loop RFID systems: A closed-loop RFID system supports a very specific process where items equipped with RFID tags are used or reused among a predetermined group of partners. These partners are usually known prior to the development of the supporting RFID system. Security requirements are very specific, as it is clear who generates and uses data of the RFID system. Typical use cases include the tracking of reusable assets between manufacturer and specific suppliers. Tagged objects are usually reusable assets such as containers or pallets that continuously come back to their originator. As the tags are continuously reused, the costs of the tags can amortize over time. In contrast to Open-loop systems, proprietary standards can be used.

Discovery Services: Discovery Services are a special type of service that is able to locate data sources containing item-level information that match a certain look-up key (e.g. EPC number).

EPCglobal network architecture: EPCglobal components (tags, readers, local EPC software stack) in combination with network access and enabling services (EPCIS, EPCDS, ONS)

Extended EPC network infrastructure: The implementation of the EPCglobal network architecture according to BRIDGE including additional business applications of BRIDGE (Track and Trace, Product Authentication, EPedigree)

Open-loop RFID systems: An Open-loop RFID system supports applications where items equipped with RFID tags are not limited to a predetermined set of partners. In such a system, we assume that tagged items do not come back to their originator at all or if so, for a long period of time for end-of-life processes. Typical use cases are Anti-Counterfeiting, Electronic Pedigree, track and trace over the complete supply chain and product lifecycle management. From a security perspective, the full set of entities, which generate or use data is therefore not known. Instead, users or data generators must fulfil certain criteria to participate in such open-loop RFID systems. This could include proofs of belonging to a certain supply chain (e.g. certified distributor for manufacturer X) or industry group (e.g. healthcare and life sciences). To achieve successful open-loop applications, open standards are required to enable seamless data exchange among participants. Tagged objects are usually individual items, which are permanently associated and identified by the EPC number on the tag.

Product Authentication: Product Authentication is simply the secure identification of a product (item). This involves acquiring, or being given the identity, and then gathering evidence and counter-evidence that this identity is correct.

Risk: includes vulnerability and a threat. The risk level is measured using two variables: likelihood and consequence of the risk.

Serial-level information: Information that refers to individual (serialized), unique items.

Serial-Level Lookup Services: Development of the Discovery Services within BRIDGE.

Threat: An event that can cause an undesirable outcome, e.g. exploitation of vulnerability.

Abbreviations and Acronyms

Acronym	Meaning
ALE	Application Level Event
ASN	Advance Shipping Notice
BRIDGE	Building Radio Frequency IDentification Solutions for the Global Environment
CIO	Chief Information Officer
CL	Contact Less
DNS	Domain Name Service
DS	Discovery Service
EAS	Electronic Article Surveillance
EEPROM	Electrically Erasable and Programmable ROM
EPC	Electronic Product Code
EPCDS	EPC Discovery Services
EPCIS	EPC Information Services
ERP	Enterprise Resource Planning
FP	Framework Programme
IP	Internet Protocol
IS	Information System
NoE	Network of Excellence
ONS	Object Name Service
RAM	Random Access Memory
RF	Radio Frequency
RM	Reader Management
ROM	Read Only Memory
RP	Reader Protocol
SAML	Security Assertion Markup Language
T&T	Track & Trace
VPN	Virtual Private Network
WP	Work Package (of BRIDGE)

1. Introduction

1.1. The BRIDGE Project

The acronym BRIDGE stands for “Building Radio Frequency IDentification Solutions for the Global Environment”. The clear objective is to enable the mass adoption of RFID for all European companies by researching, developing and implementing solutions and removing barriers. One of the main strengths of RFID technology is “its universal applicability to almost any industry, in almost every step of the value chain” [5]. However, currently deployed RFID solutions are mainly non-standard, closed loop systems that can operate either within a company or only across a small group of supply chain partners. Because of costs, the tagged objects are usually limited to reusable assets such as containers or pallets. However, for many business cases this is not sufficient. The goal is to deploy RFID also in open loop cases, as is the case for barcodes, to unleash the full power of the technology. Individual items are permanently associated and automatically identified by the EPC number on the tag. BRIDGE aims at building the hardware and software infrastructure (with regard to various industries) that is required for this next step in the RFID evolution.

1.2. Goals of this report

The work package “Security” (WP4) has the important task to provide a security framework for the hardware and software solutions developed within BRIDGE. This deliverable D-4.1.1 is part of this security framework and provides a review of the current state-of-the-art in RFID security, and states high-level security requirements relevant for enabling open and collaborative RFID-based business applications. The goal is to outline security concerns and requirements for the transition from closed loop to an open loop RFID infrastructure that should be developed within BRIDGE. In order to reflect the broad scope of BRIDGE, selected organizations of various industries were interviewed and the key, basic scenarios for BRIDGE were established. The consortium of WP4 derived security requirements and recommendations for the different layers of the targeted RFID infrastructure, based upon a proven methodology. According to the description of work, the target audience should mainly focus on the hardware, software and business work packages inside BRIDGE. The authors believe that the discussed topics are also relevant for other members outside BRIDGE to raise the security awareness and requirements concerning an extended EPC network infrastructure.

1.3. Relation to other deliverables

Inside work package “Security” (WP4), the report on security analysis and requirements represents the first document out of three deliverables. The next deliverable D-4.1.2 is planned for month M12. It will comprise a model to assess security risks associated with solutions. The work carried out by all other subtasks of WP4 will be documented in a joint deliverable. In contrast to the first two deliverables, the joint security report will focus on

solutions, guidelines and concepts to implement a secure extended EPC network infrastructure.

1.4. Structure of this document

The report is structured as follows. Section 2 introduces the overall approach that was used to establish the security analysis, requirements and recommendations. It introduces the basic methodology that was used for the interviews and the requirements elicitation process. Section 3 provides a security analysis of the current state-of-the-art and outlines the limitations of existing technologies in comparison to the open loop infrastructure that is developed in BRIDGE. The interviews (Section 3) and key scenarios and use cases (Section 5) used this gap as focus to gather a solid basis for the requirements elicitation process. Section 6 presents the requirements and recommendations according to the layers of the extended EPC network infrastructure. The report is rounded off with concluding remarks in Section 7.

2. Approach

2.1. Overall process model and organization

The goal of this report is to assess and anticipate the security needs of the various business work packages as an input for enabling open and collaborative RFID applications based on the infrastructure developments of BRIDGE. In particular, BRIDGE extends and develops the EPCglobal network architecture, especially the Discovery Services, to serve as a basis for the business work packages. Figure 1 illustrates the overall process towards security requirements and recommendations. The figure consists of a set of activities and results that are connected with each other. This document contains descriptions of the main activities (interviews, scenarios, and requirements elicitation) and presents the outcomes as sections of this report. Figure 1 illustrates which result relates to what section of this report.

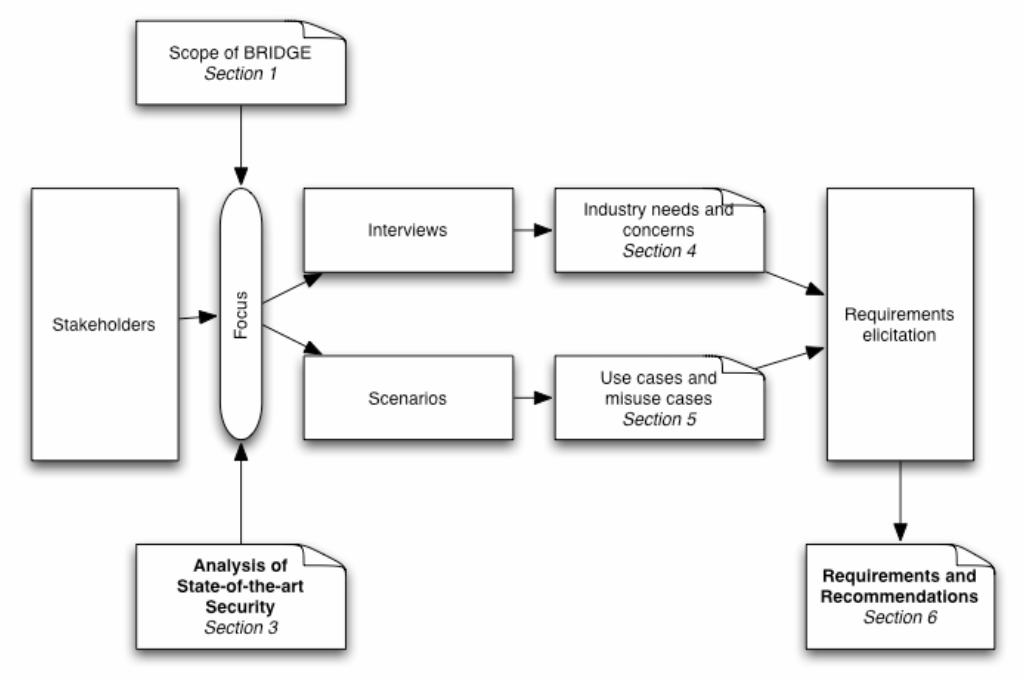


Figure 1. Overall approach

By using literature reviews, we analyzed the security of state-of-the-art EPC infrastructure and compared it with the BRIDGE objectives. The security aspects of the development challenges constitute the focus for this report (section 3). As key stakeholders for the security perspective we identified the following groups:

- Members of business work packages of BRIDGE
- Members of technical work packages of BRIDGE
- Representatives of external end-users from different industries (CIOs, Managers, …)
- Experts within security work package WP4

As the research focus of BRIDGE aims at solutions that are not implemented yet, we used a two-fold approach. First, we conducted interviews with organizations of different business sectors to collect their security needs and concerns for establishing the new solutions (section 3). Second, we created scenarios in dialog with Work Package WP2 “Serial-Level Lookup Services”, which provides a foundation technology for BRIDGE, and with WP5 “Anti-counterfeiting business application”, which represents a security application, as expert base to derive requirements from. Based on the two kinds of input, work package WP4 established use cases and misuse cases (Section 5) to derive requirements according to a selected and proven methodology (Section 2.2). The results are described in Section 6 and represent the security requirements and recommendations for different layers of the extended EPC network infrastructure.

An assessment of secondary literature revealed that the BRIDGE project is a first-mover that develops an infrastructure that enables global collaboration and open-loop business applications based on RFID data. Major security reports such as [6] and [7] focus on local deployments of RFID or closed-loop constellations. However, they indicate the attractiveness of open-loop applications [6]. Generally, there is a public belief that with on-going standardization, open-loop cases can be very attractive for the industry. Therefore, the idea was to externalize this knowledge with regard to security concerns and requirements directly from the primary source, namely the different organizations.

2.1.1. Goals

The concept is to collect the knowledge from experienced industry partners by externalizing their (partly tacit) knowledge about security concerns and requirements that are relevant for further development of their business. To reflect a common and representative view of the whole industry that could be affected by BRIDGE, requirements and concerns are collected from different industries.

2.1.2. Data gathering strategy

To fulfil the goal of assessing requirements of multiple industries, the choice was between web-based surveys or interviews as the method for data gathering. However, the idea of the web-based survey was discarded as the knowledge refers to a potential solution infrastructure in the future rather than to experience with existing systems. So, instead of a quantitative approach, the data gathering strategy focuses on the qualitative exploration of knowledge. Therefore an approach of explorative expert interviews was deemed appropriate. The interviews were conducted by experts within WP4 of BRIDGE that have both, knowledge about the intended infrastructure and about the security domain. To support the explorative character, the mode of the interviews was mainly face-to-face and partly by telephone. All interviews were conducted by the same parties and are therefore comparable. The basis for the interviews was a guideline that sets the focus for the interviews. This guideline was created in a collaboration of all WP4 members.

2.1.3. Profile of the target group

The target group was selected on the basis of several criteria. Organizations have been selected due to their general affiliation with RFID. It is important that RFID plays or will play a major role in the organization. To achieve a balanced mixture of different industry sectors, the requirement has been set that at least one company related to the topic of each business work package of BRIDGE has to be interviewed. Organizations outside BRIDGE have also been interviewed to complement the findings and ensure a broad basis. Concerning the interviewed persons of the organizations, they should be managers that are familiar with the topic of RFID and knowledgeable in security. Normally, as risks and concerns are part of the management business, this focus makes sense. Ideally they are already experienced with trials or live applications of RFID systems.

The following list summaries the profile requirements:

- Organizational RFID Experience: yes
- Broad range of industry sectors: BRIDGE WPs (must), all other (optional)
- Geographic presence of organization: Europe, Worldwide
- Interview Partner: Security aware and familiar with RFID
- Typical position: Senior management/CIO

2.2. Scenarios/Requirements methodology

Along with conducting interviews, we also follow the approach of considering use case scenarios in which the extended EPC network infrastructure will be utilized and the possible ways in which malicious users can jeopardize the system. The motivation behind using this approach is two-fold. First we tackle scenarios that are derived from what will be real applications of the upcoming architecture trying to intentionally imagine what security problems and threats will be faced. Second, with a common set of reference scenarios across the work package, the different WP tasks will have a common ground to work on, a common vocabulary, and common use/misuse cases from which they can derive different security requirements according to their interests. In the rest of this section we will describe the methodology used to derive security requirements from use-case scenarios. Description of the scenarios used will be detailed in section 5. The methodology used is based both on a number of papers [22, 23, 24, 25] that describe how to elicit security requirements by considering use/misuse cases.

We first give a narrative description of each scenario, with the required background and assumptions if any. The narrative can be divided into different scenes, which are the scenario's building blocks. From this description we derive a use-case diagram that summarizes the narrative in one picture. This picture will include the main (licit) stakeholders and the actions, which constitute their main scenes. Then the requirements extraction part begins with the definition of possible misuse cases that a malicious actor can carry out to jeopardize the system. These misuse cases threaten the described scenario and they require

certain security requirements to mitigate them. These requirements can be typically derived directly from securing the use cases. This results in a complete use/misuse case picture.

3. The BRIDGE Architecture and Current Security Capabilities

3.1. Architecture Overview

BRIDGE is based on an extended EPCglobal architecture. WP1 “Hardware” is extending the capabilities of tags and readers. WP2 “Serial Level Lookup Service” is developing missing capability in the current EPCglobal architecture. This focuses on the development of a Discovery Service to allow the location of EPC information repositories operated by other supply chain participants. WP3 “Serial Level Supply Chain Control” is developing common supply chain capabilities that use current and future EPCglobal standards and underpin end-user applications, while the business work package cluster is developing end-applications within pilot activities.

For the purposes of security analysis and technical development, we divide the BRIDGE architecture into four layers, shown in Figure 2. The diagram also shows the main focus for the combined technical work packages of BRIDGE. There is little development of the event collection and information storage pieces of the architecture as these have already been subjected to concerted standardisation efforts within EPCglobal. The effort within BRIDGE is targeted to reduce the barriers to tag and reader deployment for new application areas, and the development of collaborative RFID networks and applications. The hardware is split into separate Tag and Reader layers with clear responsibilities over hardware components and interfaces. The Network layer deals with the EPCglobal standard components and interfaces within the local and wide-area network. Within the local network we have RFID event collection and processing through the combination of the Filtering, Collection and Capturing functions. This part of the network is largely protected by traditional Intranet security techniques. Within the wide-area network we see the exposed ECPIS Query Interface, along with enabling RFID services such as the Object Name Service (ONS), Discovery Service, and supporting security services such as the Subscriber Authentication function of the EPCglobal architecture. Within this network, collaborative network security is key, as companies share sensitive information and operate business processes on data from supply chain partners.

The fourth layer is the Application layer. Applications that constitute this layer use the capability defined by EPCglobal standards to operate business activities. Such applications can be divided into two groups. The first group is applications that operate to provide common services to a number of different end-applications and companies. Such applications might provide a common track & trace capability or product verification. The specification of this common intelligence is being addressed by WP3. The second category is end-applications that sit within individual companies, as developed within the business pilot activities.

The current security capabilities within each of these layers are discussed in the following sections.

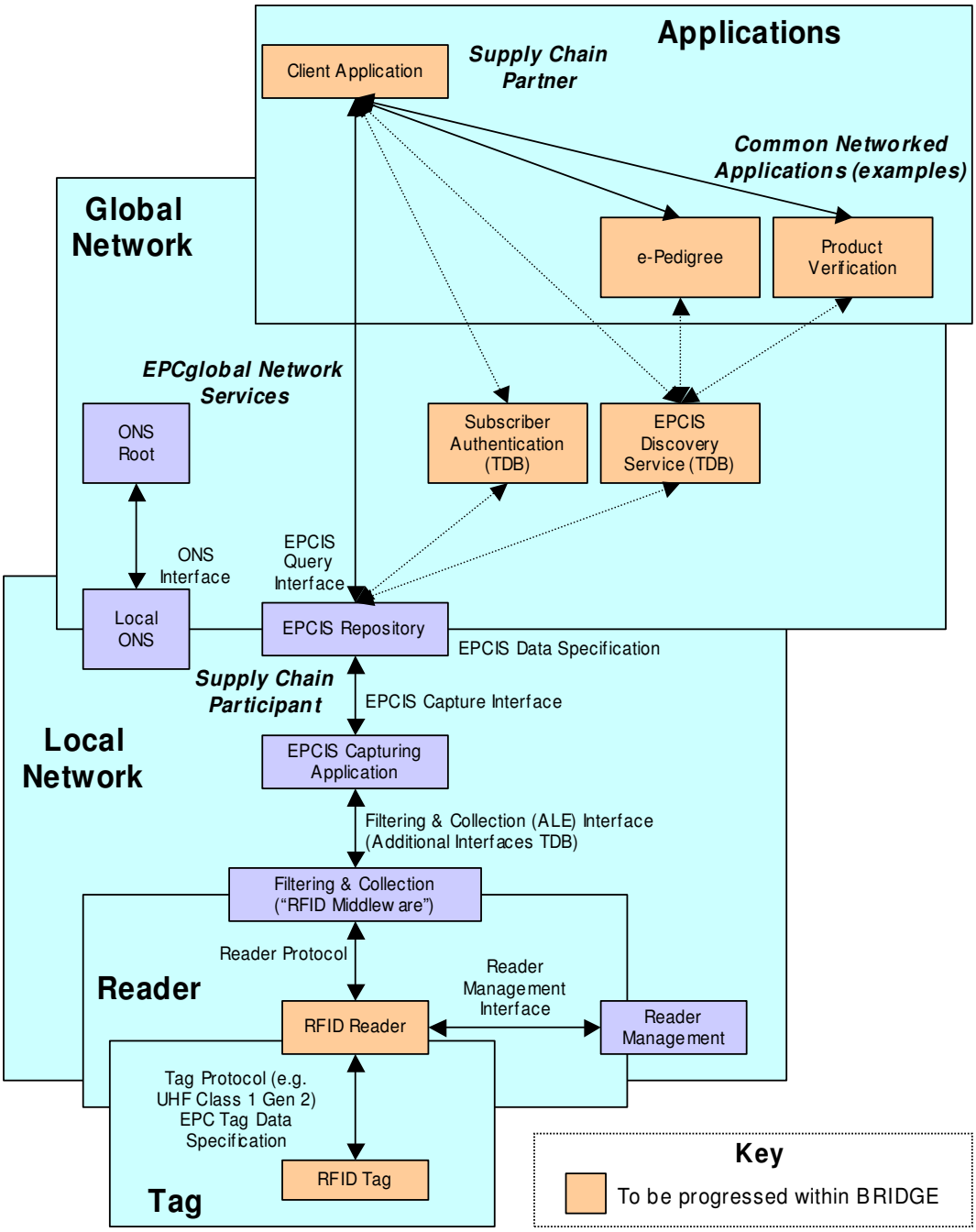


Figure 2. Extended EPC Architecture

3.2. The Tag Layer

3.2.1. Definition

Following the definition of the RFID Journal, an RFID tag is *"a microchip attached to an antenna that is packaged in a way that it can be applied to an object. The tag picks up*

signals from and sends signals to a reader. The tag contains a unique serial number, but may have other information, such as a customer's account number."[1]

A tag consists of three main components:

- Package: The package of a tag can include a so-called bolus (small glass tube for injection into farm-animal), buttons and low cost label-type packages. The most important focus for BRIDGE WP4 is the low cost, high volume packaging for mass application.
- Antenna: The antenna is responsible for reception and transmission of the communication signals between tag and reader and for collection of the energy out of the EM-field to power up the electronic circuit on the tag. Especially in UHF technology, tag-antenna design is crucial for the reading range that can be achieved.
- Silicon: A small silicon chip includes all the electronic circuitry providing the functionality of the tag. The on-chip electronic circuitry can again be divided into three separated subsystems:
    - Receiver/Transmitter (or analogue part): This part of the electronic circuit is responsible for reception and transmitting of the analogue EM-signals and transforms them into a power supply and digital signals for further computation on the tag.
    - Digital circuitry: Is responsible for execution of the communication protocol and additional tag functionality. Security features are based on cryptographic algorithms executed by the digital circuitry.
    - Memory: A tag contains two types of memory: a non-volatile memory (EEPROM) to store information that needs to be recorded when a tag is not powered (e.g. the unique ID) and volatile memory (RAM) to be used during computation on the tag.

Although EPCglobal has specified standards for Class 0/1 passive tags, active tags are available in the marketplace using different protocols and readers. While active tags do have their own power supply for operation, passive tags do not have an on-board power supply (battery) but draw all their power for operation and transmission of signals from the field a reader provides. Passive tags are therefore not able to transmit signals without the active carrier signal from a reader therefore they cannot actively initiate communication. WP4 of BRIDGE focuses on passive tags. Semi-passive tags do have a power source, but use power only for operation of their circuits (e.g. sensor logging) and not for transmission of signals. From a reader's perspective semi-passive tags act like passive tags. In the context of BRIDGE WP4, semi-passive tags provide a useful tool to implement prototype platforms with general processors that can be programmed with different security protocols.

We also need to distinguish RFID tags from contact-less smart cards, which have similar functionality (they can also provide identification via an RF interface), but are designed to meet different requirements. Since RFID tags are intended for mass production, their cost is

[1] Definition taken from http://www.rfidjournal.com/article/glossary/3#137

very crucial. Contact-less smart cards are used in applications with high security requirements, justifying a completely different market price segment. Thus, the functionality of RFID tags needs to be limited to the absolutely necessary features to keep costs at a minimum. Also, the requirements for reading distance are completely different for RFID tags and smart cards. While supply chain applications require reading distances of 1 meter and more, a typical application for CL-smart cards has a reading distance of a few centimetres. This short reading range actually enhances the security of such smartcards. For the design of tags this means that the energy consumption of the tags is absolutely crucial, since it limits the operating distance. We can assume that the energy available for an RFID-tag operated at maximum reading distance is about 1/1000 of the energy a typical CL-smart card.

3.2.2. Current Security Capabilities

Current supply chain applications do not make use of security measures for the tag-reader communication or for the information stored on tags. Many current applications of RFID tags operate in constrained physical environments (such as warehousing and logistics) and do not have special requirements for protection of the information. If tags are operated as a substitute for bar codes and only used in environments that limit physical access and eavesdropping, then additional security will bring a benefit to these applications. Within BRIDGE we seek to provide additional security at very low cost to enable the use of RFID to spread beyond these protected boundaries. Current specifications of passive tags do allow the use of passwords to control the operations (for example writing or killing) of the tag. However, the security of such simple passwords is low, and the cost of managing these passwords is significant.

Although the majority of tags are used in applications without security requirements, some applications with enhanced security functionality exist. Tags designed for such secure applications are generally active (e.g. car immobilizers). They typically use proprietary crypto algorithms (mostly stream ciphers) and undisclosed protocols that prevent security review and economic deployment across multiple organisations. Latest investigation on the security of current stream ciphers in the FP5 project NESSIE[2] revealed security flaws of many stream cipher primitives. In the currently running FP6 NoE ECRYPT[3] an activity on investigation of new stream cipher primitives is currently ongoing. So far, the security of stream cipher primitives suitable for application on RFID tags is treated as uncertain.

The price of tags heavily depends on the silicon area of the chip. In current semiconductor technology used for RFID tags, the basic functionality of the tag uses all the available silicon area to allow tag production at an acceptable price. Smaller silicon technologies will dramatically reduce the size of the components providing the basic functionality (protocol execution and memory), but production does not allow the fabrication of chips smaller than a certain size (e.g. handling of smaller chips is more expensive). This means that “additional” area for security functionality is available without increasing the price of future tags.

[2] https://www.cosic.esat.kuleuven.ac.be/nessie/index.html

[3] http://www.ecrypt.eu.org/stream/

The data protection party of the European Commission[4] analyzed RFID technology in the context of "Data Protection". They investigated how RFID systems need to be implemented to comply with European Data Protection Laws. In their working document on "Data protection issues related to RFID technology" (currently under consultation[5]) they state that when RFID tags contain personal data, they must provide technical measures to protect this data from unauthorized access. Please note that under the European Data Protection Directive, 'personal data' is very broadly defined and includes *"any information relating to an identified or identifiable natural person"*.

3.3. The Reader Layer

The advantage of RFID technology over earlier technology, such as optical barcodes, includes the ability to identify objects without line of sight. However an RFID system is not only comprised of tags. Any benefit relies on a system capable of acquiring data from the tag and transforming the data into useful information for specific business processes. In this section we consider the security requirements for the RFID reader.

3.3.1. Definition

RFID Readers are devices that communicate wirelessly with the RFID tag to identify the tag identity or in certain cases to read other information stored in the tags (such as sensor readings). RFID Readers are also capable of writing information to the tag. We can consider the reader as possessing two types of interface:

- *The radio interface*. An important characteristic of the reader is the radio interface standard that includes the power output, the radio frequency over which the reader can operate, the singulation and the communication protocol. In BRIDGE, we mainly focus on the EPC C1G2/ISO 180006C standard but we will also consider other tags and protocols for specific research tasks.

- *The network interface*. Another important aspect of an RFID reader is the interface that enables communication with the enterprise systems. The reader can filter and aggregate data and support specific enterprise components (e.g. a distributed messaging platform). The reader is the first point of data injection into the supply chain. It is therefore crucial that a reader is a secure and trusted device.

3.3.2. Current Security Capabilities

Although other reader devices exist, particularly for active tag technology, WP4 considers the evolution of readers within the EPCglobal architecture. These readers have been designed to support the reading requirements for simple passive tags. Task 4.4 of BRIDGE is therefore concerned with developing the reader further to enhance the security features when the

[4] http://ec.europa.eu/justice_home/fsj/privacy/

[5] http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm#wp105

reader is used with the existing tag specifications, and also to provide a reader platform that is capable of working with new tags with security functions developed in tasks 4.2 & 4.3.

The security of the radio interface is defined by the tag specification that is being read. Most tags (e.g. EPC C1G2) do not provide authentication to the reader, so the reader will accept whatever identifier or other memory values that are provided by the tag. These values are not processed by the reader, but passed to the host for collection and processing, limiting the facility to perform attacks on the reader by this interface.

On the network interface, the EPCglobal Architecture defines a Reader Protocol (RP) interface and a Reader Management (RM) interface. The Reader Protocol specifies Command Channels for issuing commands to the reader and Notification Channels for the return of events from the reader. In addition, the Reader Management specification also defines Alarm Channels.

When establishing one of these channels, the host performs a handshake with the reader to negotiate message and transport bindings. Transport bindings may include encryption and authentication. An example of a secure transport binding is HTTPS, although the reader vendor may add other secure transport bindings. Once connected, the Reader Protocol allows the use of passwords to control access to the tags, where the tag protocol supports access or kill passwords. We are beginning to see RFID reader vendors offer such authenticated binding for interaction with and management of their readers, including encryption of the communication.

The EPCglobal Architecture also specifies RFID middleware offering Application Level Event (ALE) and other yet unspecified event collection interfaces. Although current implementations offer this functionality external to the reader, in the future we may see such capabilities and interfaces provided on the reader hardware. Thus one activity within task 4.4 is to support secure open services on the reader platform. As with the RP and RM specification, the ALE interface may be offered through a number of different transport bindings. The expected Web Service/SOAP binding could use HTTPS as well as using elements of WS Security. Other message-based transport bindings such as JMS or MQ can similarly provide authentication, access control and encryption.

3.4. The Network Layer

3.4.1. Definition

For the purposes of BRIDGE, we define the scope of the RFID network activity to extend from the RFID collection infrastructure, through the single authority information systems, to the multi-party RFID co-ordination networks. In the terms used by EPCglobal this means the EPCIS capturing applications and repositories, along with Object Name Service (ONS) and Discovery Service (DS).

These components of a local, and extended, RFID information network will commonly operate over existing IP based intranets, VPNs and the Internet. Those components that sit

within an organisation such as the collection, filtering and capture components are assumed to sit within a secure IP network that provides the first layer of defence. Furthermore these components are largely already standardised, and the interfaces are expected to use existing authentication mechanisms and secure transports already deployed within the organisation. Security technology decisions made within one organisation do not impact directly on partner organisations (except to affect the level that that partner can trust the information).

In contrast, within the wide-area network we need common security capabilities to enable the inter-working of multiple organisations. Some components are already standardised while others are still largely work in progress. The EPCIS is close to being standardised, while the ONS has existed for some time. Thus, the effort in WP2 “Serial-Level Lookup Service” is to develop the main inter-company serialised-level lookup service - the Discovery Service. The secure design of a Discovery Service is essential to its success, as parties will share information with external organisations. The Discovery Service should act as a secure trusted intermediary between the operator of the EPCIS and the client application searching for EPC data.

Crucial to the success of collaborative RFID networks is a common security framework that governs the access to all shared interfaces including the EPCIS and the Discovery Service. How such access policies are defined and enforced within this collaborative RFID network is the key concern of task 4.5 of BRIDGE.

3.4.2. Current Security Capabilities

The latest EPCIS candidate specification allows multiple technology bindings of the EPCIS Query Interface. Unlike the lower level interfaces, EPCIS specifies that the binding *must* provide a means of mutual authentication between the EPCIS and the client. This authentication is used to determine authorisation and perform access control. The earlier ONS specification makes no mention of security on the registration or query operations, being implemented upon DNS (Domain Name Service), and reachable through the DNS network. Largely the ONS information is not considered highly sensitive since it typically (or initially, at least) refers to class level information from the manufacturer of the product. If a more secure ONS is required, some material has already been written on the application of DNSSec to ONS. This would provide ONS with greater security in terms of the integrity of the information records. Publishers and ONS servers would authenticate before passing signed information records. DNSSec would not address any concerns over the confidentiality of records as DNS is designed to publicly share the addresses of network devices.

The EPCglobal architecture also defines the role of EPCglobal Subscriber Authentication, although this function has yet to be implemented. For the purposes of BRIDGE, authentication of only EPCglobal subscribers is insufficient as many operators and users of components in the BRIDGE architecture (and indeed of components in the EPCglobal architecture) will not be EPCglobal subscribers. Instead, the authentication of EPCglobal subscribers should operate alongside many other authentication services for the purpose of accessing RFID network components and higher applications. Clearly there are existing major initiatives around identity authentication such as Microsoft’s Passport and Liberty Alliance. RFID systems should operate within the framework of these systems to enable

applications to easily use both RFID and non-RFID services. The use of a cohesive authentication system can also enable Single Sign On between different components of the wide-area RFID network. This is particularly powerful if client requests are relayed between different systems using an assertion language such as SAML.

Credentials may not only specify identity, but also roles, groups or resource access rights. Since open multi-party RFID networks have yet to be implemented it remains unclear what assertions should be made to gain access to different RFID resources and facilitate scalability and management.

Once parties' credentials have been checked, we also require security policies to control the operation of components in the architecture. The EPCIS specification does not detail how such authentication is performed, or how such security policies are constructed. Since the construction of such local policies is internal to an organisation no standards are required and vendors are free to compete over such security features. However, such arguments do not apply if we consider how a company's security policy can be implemented over a number of components including their EPCIS and one or more Discovery Services. Clearly having different policy structures on each component will lead to higher administration costs and inconsistencies that could lead to security flaws. Standard methods of describing access control policy languages such as XACML can clearly help in this area.

3.5. The Application Layer

3.5.1. Definitions

Within the scope of BRIDGE, the Application Layer encompasses three major applications that support shared business operations. These applications use components in the Network Layer such as the Discovery Service and EPCIS Query interface to construct the data they require to enable the business process. The following sections will describe each of these applications

3.5.1.1. Track and Trace Application

The *Track and Trace* application uses the Discovery Service to identify the EPCIS systems that handle a product. Requests to those EPCIS systems can then elicit more detailed track & trace information such as shipping times, delivery methods, and aggregation information. These details can then be used to build historical models of the supply chain network that can then be used to both query product trace history, along with handling queries about a product's future. For example, the model might suggest that a certain class of goods normally takes 2 days to arrive at the retailer after dispatch from the wholesaler.

Constructing such detailed models requires potentially sensitive information to be shared by the members of the supply chain, although it is feasible to decompose this model into local subcomponents that can be operated by individual members of the supply chain or more localised trace & trace services. Such local processes can minimise the risks of sharing

confidential information, although in turn we require the ability to ensure that such processes are executed correctly.

3.5.1.2. Electronic Pedigree Application

An *Electronic Pedigree* (ePedigree) provides evidence of a product's chain of custody. Typically, this will detail the arrival and departure times of the product through each of its supply chain partners, and can be created either on-demand or pre-emptively via secure trace and trace queries. Essential security elements of an ePedigree are its integrity and non-repudiation. In certain cases, confidentiality and even a degree of anonymization[6] may also be required. Guarantees of non-repudiation can be achieved using different mechanisms. Sharing the data with a trusted third party could be one approach, however, this requires duplication of the data, and compromises the confidentiality of the publisher. Other cryptographic approaches may provide a better balance between all the security requirements of the actors in the process.

3.5.1.3. Product Authentication Application

Product Authentication is about gathering evidence that a claimed identity is authentic, and then presenting that information in such a way that a decision on its authenticity can be made. More formally, we can test one of two null hypothesis (which are each other's alternative hypothesis). Either:

- the product is indeed authentic, or that
- the product is non-authentic (incorrectly claiming it's identity). Counterfeit products are a dominant example of products in this class.

The tests and evidence are used to distinguish between these alternative hypotheses. However we must be aware that the test could produce the wrong result: false positives and false negatives.

		Authenticity Test Result	
		TRUE test suggests it's authentic	*FALSE* test suggests it's non-authentic
Actual Product Authenticity	*AUTHENTIC*	Truly Authentic	Falsely Non-authentic (false negative)
	NON-AUTHENTIC (esp. Counterfeits)	Falsely Authentic (false positive)	Truly Non-authentic

A critical, pragmatic, feature of Product Authentication is to construct the tests in such a way as to best suit the client's needs. [Different clients may have different fundamental objectives, and be prepared to pay different costs according to their location in the supply chain]. The primary characteristics that can be varied in creating an Authentication test is:

- the types of evidence gathered
- the granularity/accuracy of the evidence gathered

[6] e.g. It may be sufficient to merely know that a valid electronic pedigree exists, without necessarily disclosing the details of each change of ownership.

- the hypothesis being tested

The relative acceptability of false positives and false negatives is a key determinant, and is ultimately a commercial decision based upon the product type and the use made of the authenticity check. For example, if it is strongly required to guarantee the authenticity of a product, then the false positives must be minimised. This can be achieved by testing against a stricter hypothesis, although the consequence is that some products will then be falsely classified as non-authentic. Decreasing false positives through better evidence will not result in more false negatives, but incurs a higher cost to the business.

In terms of information confidentiality we must consider what evidence is collected and who performs the tests. It is feasible that in some cases such tests can be decomposed and operated over localised evidence, allowing better control of sensitive information.

Finally we must consider how the test results are presented. This includes the extent to which the hypothesis has been proved and confidence in the result. In returning such information we must consider the recipient, and the potential disclosure of sensitive information. For example, we may only wish to give an authentic/counterfeit response to an end consumer without the evidence used to derive the result.

3.5.1.4. Product Verification Services

Product Verification is the process of checking that a particular item is 'valid'. This comprises of a combination that the item is authentic (that we can attest the identity), along with other checks that meet the requirements of the business process. One example might be to combine an authenticity check, along with an ePedigree check to ensure that the product has met certain supply chain constraints. Other checks might include that the product has not exceeded a temperature threshold, has not passed beyond a sell-by date, or has duty paid.

As with the other applications, these checks require sensitive information to be released by different supply chain partners. Any solution should be designed and distributed carefully to minimise these concerns. Where pedigree or sensor data is carried along with the tag, we must also consider the transfer of information between businesses via the tag, and attacks that compromise the data on the tag.

3.5.2. Current Security Capabilities

The common shared applications that we have been discussing do not largely exist, although parallels can be drawn to existing business hubs, such as electronic marketplaces and secure message exchanges such as EDI. However, many of these systems are centralised under the authority of a dominant player, or entirely internal to an enterprise. As such they assume high levels of trust in the application provider, and rely on perimeter security (e.g. VPNs) to meet their security demands. Moving these applications to a highly distributed open environment means that they are exposed to new threats (such as Denial of Service attacks), and must not rely on network security. It also means that security has to be based on standards wherever possible to reduce the cost and complexity of authentication, access control and encryption.

Security concerns for these applications are around the integrity of the processes (including aspects of data integrity and service availability), along with leakage of business intelligence (confidentiality and user privacy). Applications built over the Discovery Service must also be keenly aware that they inherit security characteristics from these lower network services. For example an ePedigree application that requires non-repudiation of product history cannot rely on this capability from the EPCIS or Discovery Service.

3.6. Identified Focus of This Report

The contribution of BRIDGE is to build a secure RFID system that extends the current EPCglobal architecture and enables global RFID processes and novel applications of RFID. WP2 is focused on designing a Discovery Service as a basic RFID network service to underpin inter-operation between loosely coupled businesses. WP3 is developing the supply chain intelligence capability such as track & trace models that will be used in shared applications. WP1 is focused on enhancing the capabilities of tags, antennas and readers to allow new applications of RFID.

WP4 largely shares these priorities. The collaborative RFID network is largely undeveloped and security is key to its success. Companies will only collaborate if they can extract value form sharing information and manage the risks to their operations. The collection and information storage pieces of the architecture largely sit within secure network and physical environments. However we envisage that the tags and readers will become increasingly exposed to attacks. New applications will also require stronger guarantees of confidentiality and integrity than are currently provided by the tag and reader pieces of the architecture.

Thus the role of WP4 is twofold. Firstly it must ensure that the RFID Network Layer is capable of allowing secure operation between multiple parties. This is absolutely key to the success of global RFID deployment, since, without appropriate security, companies will continue to build silos of RFID information and many valuable applications will be impossible. The second role is to build security functionality into the tags and readers to enable applications that rely on security. These might be applications where the RFID information is considered confidential, or in many cases where the RFID information (or the lack of it) can be used to stall or subvert critical business processes. An obvious application is tags that can provide product authentication to support applications such as anti-counterfeiting. However, we must be aware that in moving from tightly controlled closed environments to multi-party open supply chains, most business processes become subject to serious threats as they rely on information from other parties. These parties may be malicious, or may simply not implement satisfactory levels of security within their own organization.

The following sections of this report contain the results of a survey into the threats businesses see in implementing global RFID systems, along with multi-party application scenarios. These are then used to determine the threats and security requirements that the architecture layers must address in WP4 to enable a secure global RFID applications.

4. Interviews

As outlined in Section 2, interviews were conducted to provide qualitative input for the security work package. The following sections detail the actual interview process and present the findings.

4.1. Target group and experience level

The target group for interviews consisted of organizations that are familiar with RFID systems and the related security concerns. Organizations have been selected on based on their experience with closed-loop RFID applications and their relevance towards the business topics covered by BRIDGE. In total, twelve companies have been interviewed in an explorative face-to-face or by telephone. The interview partners were mainly CIOs or Senior Managers. Figure 3 shows the number of organizations that gave input for security concerns in specific business applications. It is evident that nearly all interviewees are experienced with live or test implementations. The group is actually divided into three clusters. Solution providers in this document are companies that offer hardware, software or consulting services to deploy RFID systems. End-users are simply all organizations that use these RFID solutions to support their business. “Other” refers to not-for-profit organizations.

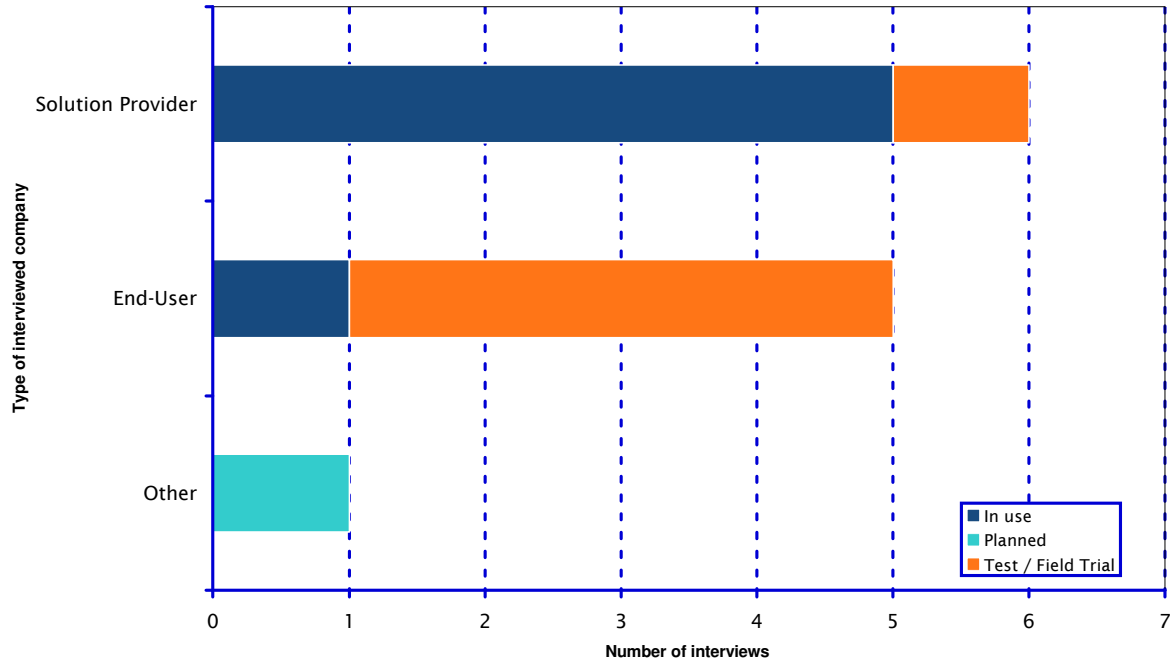


Figure 3. Interviewed target group and experience level with RFID solutions

4.2. Coverage and relevance for BRIDGE work packages

All the business work packages of BRIDGE (WP5 to WP11) are covered by interviews. Figure 4 shows the number of interviews that are relevant for each corresponding work package. As Anti-Counterfeiting and Drug Pedigree are very new applications that are currently being developed and adopted, they are just covered by interviews with solution providers. In contrast, for other business applications like “Textile Supply Chain Management”, “Manufacturing”, “Re-usable Asset Management”, “Products in Service”, and “Item-level tagging of non-food items”, a number of important End-users could be found. Beyond the scope of BRIDGE, additional business applications like “Animal identification” and “Port security” were covered. *Note that most of the 12 interviews covered multiple topics addressed by BRIDGE work packages. For example, one interviewed manufacturer in the textile industry provided input relevant for WP7, WP8, and WP11.*

	Description	Solution providers	End-users	Others
WP5	Anti-Counterfeiting	3		
WP6	Drug Pedigree	3		
WP7	Textile Supply Chain Management		2	
WP8	Manufacturing		2	
WP9	Re-usable Asset Management	3	3	
WP10	Products in Service		2	
WP11	Item-level tagging of non-food items	3	2	
Other	Beyond the scope of BRIDGE (animal ids, port security, ...)	3		1

Figure 4. Coverage of BRIDGE Work Packages by Interviews

4.3. General comments of interviewed group

The interviewees that talked from experience with their RFID applications do not see big security problems in their current implementation. The reason is that they use RFID mostly in closed-loop systems. Point-to-point VPN tunnels and general IT-hardening measures are therefore sufficient. Some of the interviewed manufacturers indicated that there is no need in their use case to move to an open-loop system, unless their main customers require them to do so. They all agree that additional security measures need to be taken when moving to an open-loop system. But not all of them see the justification for higher tag prices. The reason is that even the current tag price is too high for tagging low-cost products. In regard to paying extra for a tag authentication service, none of the responses was positive toward the idea of spending extra money. The reasons for investing more in RFID security would only be if a clear business case existed or a higher functional feature set on the tag. For example if Electronic Article Surveillance (EAS) functions can be integrated within the RFID tag, higher costs can be justified.

4.4. Security concerns

The companies were asked to identify their top three security concerns in the RFID use case(s). The stated concerns were ranked to reflect their priorities. Hereby primary concerns indicate high priority whereas tertiary concerns are of lower priority. Figure 5 shows the share of each concern. It should be noted that this data only reflects the results of this study and cannot be generalized e.g. as the overall importance of these security concerns. Although parties were able to give straight answers on this high-level question, a more detailed insight to the threats that relate to the stated concerns was only given by examples. The reason is that most managers cannot translate these concerns directly to technical security requirements or that the technical requirements are still unknown. Therefore, the concerns explained in the following sub-sections (4.4.1 - 4.4.9) reflect only the business perspective in regard to the security requirements. The technical perspective is provided later in Section 6 and it provides requirements for the specific RFID layers to mitigate the stated concerns.

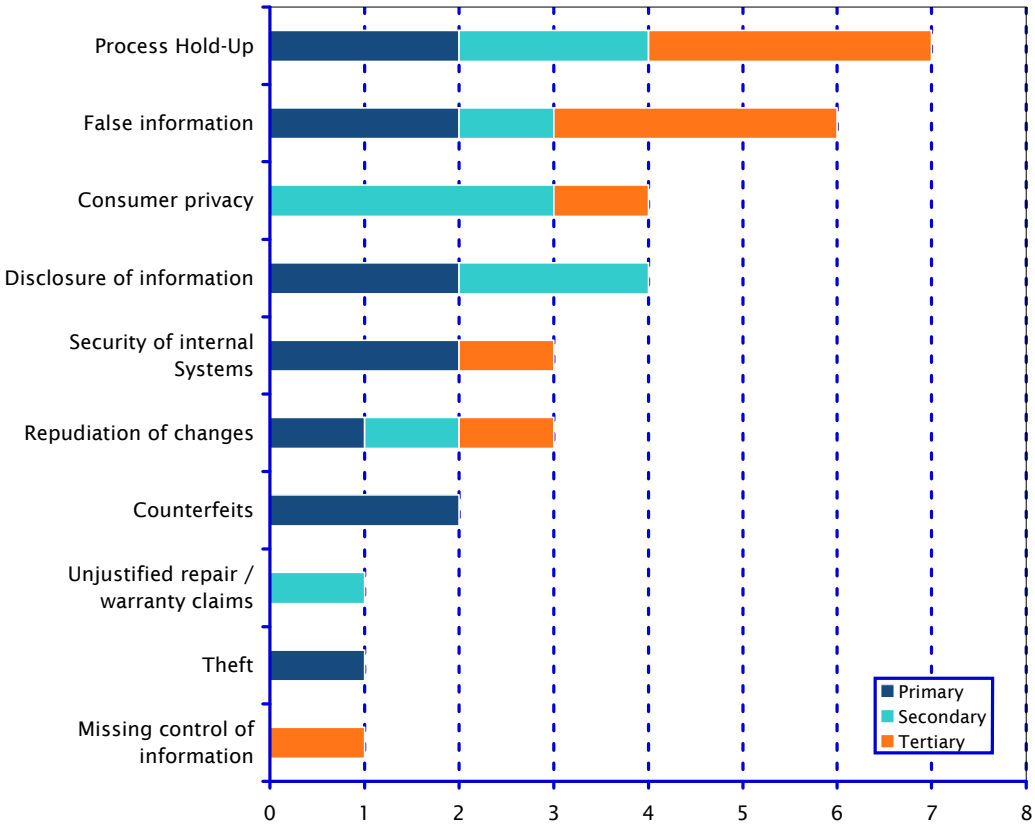


Figure 5: Security concerns for doing business over an open-loop RFID system according to the response of the target group

4.4.1. Disclosure of confidential information

According to the responses, disclosure of confidential information is among the biggest security concerns for organizations. When moving from closed to open loop, data is not

within the control of the company. The type of data that is going to be shared within the EPC Network is the critical factor. Especially when EPC numbers can be related to a product catalogue or other information system, the potential of abusing this data is very high. For example a company can gather confidential data to reveal new target groups and markets for the products of its competitor. Track and trace data can be abused to reconstruct the strategic relationships of a company and identify its important partners and channels. Also the identification of the most important supply routes or the exact locations of high-value consignments would impose a risk that criminals can target their harming illicit endeavours in a more efficient way.

4.4.2. Security of internal IT-Systems

As companies open their IT-systems for information sharing and access to EPC network services, their internal IT-systems become more vulnerable to attacks from the network. Most importantly, companies will transact with bigger number of partners and these partners might be unknown beforehand. Also, vulnerabilities of readers impose a risk if they are directly connected to the IT-system, in terms of blocking, exploiting, or damaging other vital systems such as ERP systems.

4.4.3. Consumer privacy

RFID can facilitate automated tracking of individual people thus threatening the consumer privacy. In reality, privacy issues that RFID poses to consumers are amplified through media coverage, actions of pressure groups, and dramatization [26]. The result is that consumers perceive privacy risks greater than they might be according to quantifiable facts. This misunderstanding, however, poses a serious threat to retailers and not addressing the issue might lead to loss of consumers trust, confidence, and fidelity. Privacy enhancing technologies such as disabling tags attached to products can be a part of the solution, though it has to be kept in mind that the problem itself is not only technical and thus also other means are needed.

4.4.4. Injection of false information

Event data of EPC enabled objects is generated throughout the whole supply chain. As this data is shared among organizations, the question of authenticity and trust must be addressed. As EPC events are the digital representation of business transactions, the EPC network must ensure that past data cannot be manipulated or used twice. To prevent malicious actors from introducing false information, injection of data and the injected data itself need to be controlled.

4.4.5. Process/manufacturing hold-up

As more and more processes are automated through RFID, the risk of a process or manufacturing hold-up increases. More real-time operations hinge on the availability of RFID data. Therefore the data must be continuously available. To ensure the availability of data and network services, the architecture must provide concepts to mitigate risks of hold-ups.

For example, if all parties rely on shared network services to determine the authenticity of products, it must be ensured that this service is always available. Also the availability of tags and readers needs to be addressed.

4.4.6. Theft

Some interviewed companies mentioned that RFID imposes threats that facilitate the theft of goods. On the one hand high-value goods can be identified in an easier way. And on the other hand, in-store thefts could increase as information can be altered to mark for example an unsold item as sold or change information that determines the sales price. The concern mainly emerges from the threat that tools for manipulating or hacking websites can be abused to alter data on a big scale in networked item databases. It should be noted that a theft prevention system is only as strong as the weakest link and so this threat should be considered not only from the point of view of RFID technology.

4.4.7. Counterfeits

The risk with using RFID to fight counterfeiting and illicit trade is seen in the way that automated checks can be fooled. For example, with adequate technology, one valid tag can be abused by cloning it numerous times to validate fake products. The RFID infrastructure must ensure that anti-counterfeiting is effective and cannot be abused on a mass basis.

4.4.8. Repudiation of changes

In contrast to barcodes that require a line of sight for reading, RFID is a technology where read and write transactions are not obtrusive. Clandestine read or write access is hereby a security concern that already emerges between tag and reader. When moving to a networked RFID platform, based on current Internet technology, a second potential area of unintended listening and manipulation of communication is introduced. The repudiation of changes is especially important if data is manipulated or if legal claims come into effect. The system architecture must therefore ensure that changes and access can be traced back to specific identities.

4.4.9. Missing control of information

When the data is used in shared network services, companies see a problem that they are loosing control of their data. It must be ensured that the way in which the data is going to be used is clear and that the possibilities to abuse it are minimized. Otherwise companies will see very high risks in publishing the product specific information and using the EPC network.

4.5. Trust in hosted security services

The following sections will focus on the aspects of security services that can guarantee identities or check the completeness and plausibility of item-level information. These services could be the basis for a security framework that all EPC network users can rely on.

4.5.1. Trusted service operators

To have a neutral security service, these services need to be hosted and fairly available to every user of the EPC network. The interviewees were asked who they would trust as an entity to operate EPC network security services. While most responses (33%) indicated that a trust for those security services would not be different from any trusted business relationship, the other interview partners had different preferences, which varied a lot. They stressed that this is highly dependant on the type of service and the type of solution.

4.5.2. Factors that increase the trust

The interviewees named a set of factors that could increase the trust in the operating company of a security services. These are as follows, in the order of importance:

- Open Standards (41%): The interfaces for data publishing, data access and identity management should operate in a standardized way so that it is clear to every participant how the data is accessed and the security services operate.
- Security certifications (17%): Participants should undergo a security certification procedure before being allowed to participate in the EPC network and to use the security-relevant services.
- One-to-one contracting (17%): While the security services may be hosted, data treatment could be subject to specific contracts that companies make with the security operators depending on the data they will publish.
- Other (25%): Other mentioned factors would be personal relationships to the operating company and the operation under the same laws. This is especially because data management guidelines may differ from country to country.

4.5.3. Risks for publishing item-level information

For some security hosted or collaborative security services like Anti-Counterfeiting or general track and trace plausibility checks, the publishing of item-level information is necessary. The interviewees were asked what risk they would see, if they make their item-related information available for the Discovery Services. As depicted on Figure 6, over 58% of the interviewees are estimating a high to very high risk in publishing their information. The most mentioned reasons for this high risk come from either a general opinion that information should never be made available if its not clear how it is going to be used and by whom. Some of the respondents were able to indicate that they are afraid of facilitating their competitors' intelligence and that this information can expose high-value consignments and location information to criminals. 33% of the interviewees are stating a medium risk, as they do not feel that this item-related information is more critical than any information that is exchanged in today's business. The remainder of 9% even claimed a low to very low risk, as pure item-information would be published without references to business contexts and is therefore useless without an additional references database.

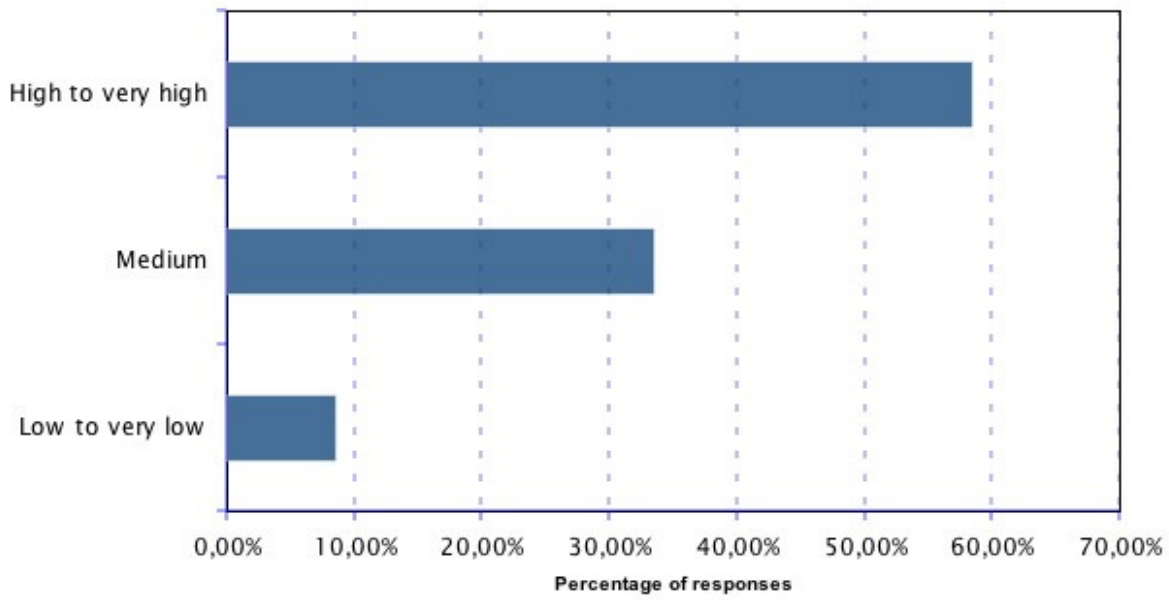


Figure 6. Risks for publishing item-related information

4.6. Conclusions

The interviewees were generally able to deploy secure closed-loop systems and were knowledgeable about security aspects. However, direct requirements could not be elicited from the interviewees, as they would need more information about the design of the extended EPC network architecture. The choice to use explorative interviews allowed to get a deeper understanding for the influencing factors of security from their point of view. This section provided a broad list of security concerns and explained why the interviewees have these concerns. The interviewees also recognized the need for central security services in order to deploy an EPC infrastructure that is suitable to run open-loop application. However, they indicate a high to very high risk connected with making their item-level information available to potential other partners. They concluded that it is not only about the process how others access data in their data pools, but more a question of knowing how the data is actually being used and by whom. Access policies and hosted security services would therefore depend on the application and the range of partners that can use them.

In summary, the concerns mostly are that high as there is no fully specified design yet. We expect that the stated concerns can be mitigated mostly by design (Injection of false information, Missing control of information, Counterfeits, Theft, Process/manufacturing hold-up), standards, physical security, policy/contracts (Disclosure of confidential information, Repudiation of changes, Consumer privacy), classic IT-security like fire walling (Security of internal IT-Systems), and a combination of these. As most of the concerns emerged from a lack of knowledge of the design and type of use, probable scenarios in the next section will help to elicit requirements.

5. Scenarios and use cases

In addition to the interviews described in the previous section, we adopt another approach to derive security concerns and requirements. In this approach we consider use case scenarios in which the upcoming architecture will probably be used. This complements the interview approach because here we directly put the EPCglobal open-loop architecture to the test by considering what we expect to be typical usage scenarios. As pointed out in the previous section, the interviewees were primarily concerned with their current closed-loop systems and did not see the need to move to open-loop systems, which makes this use-case approach all the more important to identify security threats that the interviewees overlooked. We detail in this section each of the scenarios that will be used to elicit security requirements and depict their use/misuse case diagrams.

Many parts of the architecture, particularly certain parts of EPCglobal, haven't been defined yet, so for these we make a few assumptions that are in line with the current discussions going on in WP2. One such assumption concerns the EPC Discovery Service (EPC DS), whose primary functionality will be to locate all EPC IS services having information about a specific EPC number. The assumption we use abstracts over the detailed implementation of the EPC DS and only assumes that the service receives a request with an EPC number and returns all EPC IS address containing information about the particular EPC.

5.1. Product Manufacturing

The manufacturing stage of a product's lifecycle is a particularly essential part since its main output, a proper tagging of an item, is prerequisite for all other scenarios to function properly. This scenario covers primarily the initialization of a product, both on the level of the physical tagging and that of the initialization of the EPCglobal records. Figure 7 shows the use case diagram, followed by a narrative explanation of the scenario, and finally we present the misuse case diagram in Figure 8.

5.1.1. Scenario Description

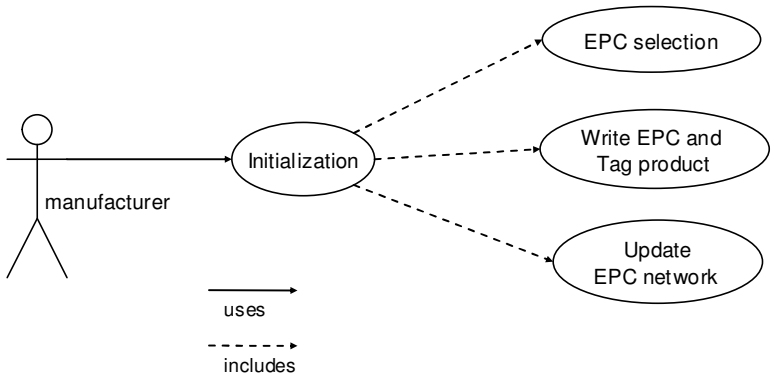


Figure 7 - Product Manufacturing Use Case Diagram

Manufacturer M produces product P. For different reasons, company M wants to tag P with an RFID chip. Reasons can include abiding by enforced regulations in P's industry branch, providing an added value for the clients of M, etc. When P's manufacturing is completed, M selects a unique EPC number to associate it with P. The number is written onto an empty RFID tag. The tag is secured as required (by regulations, industry, etc) and gets physically attached to the product. From now on the tag should never be detached from the product under normal conditions. The next step is to update the corresponding information systems and inform them of the new product and its EPC number. Company M's EPC IS repository is updated with the newly created EPC. The company also notifies the EPC DS through a message that contains the EPC number and its host EPC IS.

5.1.2. Misuse Cases

Figure 8 shows the misuse case diagram for the product manufacturing scenario. Each terminal bubble in the use case diagram can have misuse cases that a malicious user or even an inattentive or careless legitimate user can commit. These can be countered by security features, checks, etc. For example the EPC selection process can be jeopardized by reusing an old EPC or one that is not allocated for the particular manufacturer. Against this we expect that security measures and procedures will be in place to ensure a unique and transparent EPC selection to mitigate the threats posed by reusing an old EPC.

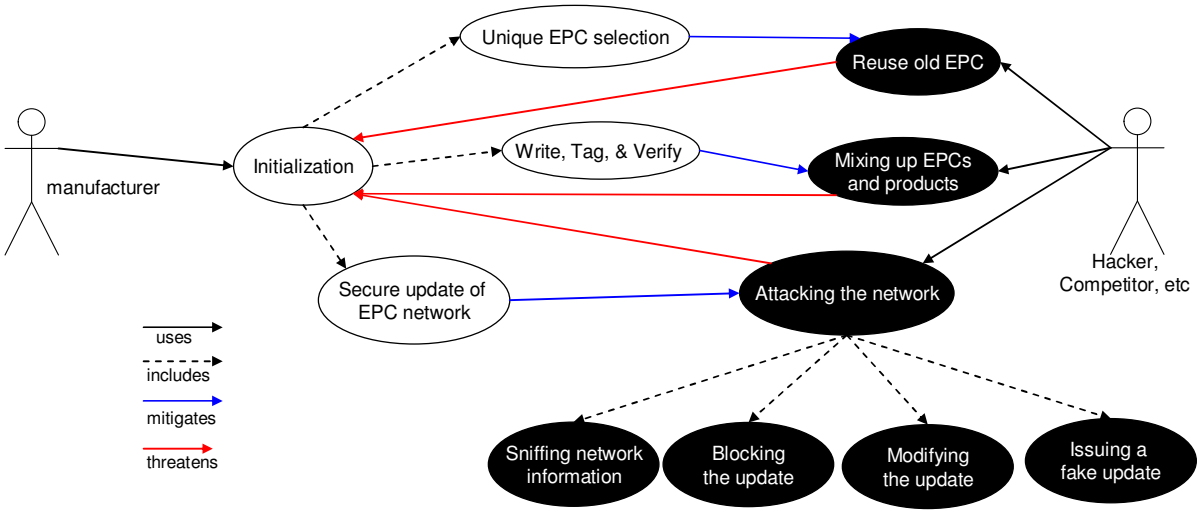


Figure 8 - Product Manufacturing Misuse Case Diagram

5.2. Product Transfer

This scenario deals with product selling and purchasing. These operations transfer the ownership of the product and may thus cause updates to the EPC network information about this product. In our generic description below we consider a wholesaler selling a product to a retailer, but the security analysis will be the same for different partners. For the wholesaler this is an outbound scenario and for the retailer it is an inbound scenario. Figure 9 shows the

use case diagram, followed by a narrative explanation of the scenario, and finally the misuse cases.

5.2.1. Scenario Description

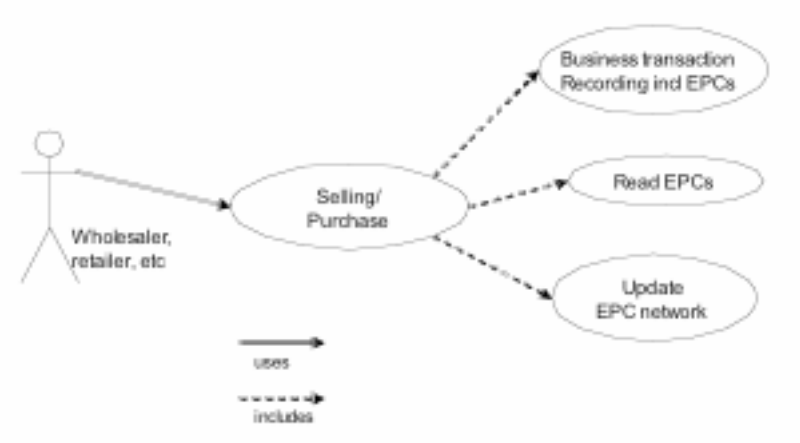


Figure 9 - Product Transfer Use Case Diagram

Wholesaler W wants to sell P to Retailer R, as part of a shipment that contains several other items and products. Before the actual shipment takes place, the business transaction is communicated between the two companies. After proper authentication and credential identification, W's business systems issue an Advance Shipping Notice (ASN) to the business systems of R. The ASN includes, in addition to the business transaction data, all the EPC numbers to be shipped and delivered. R's ERP system then provides its EPC IS capturing application on the shipment site with the expected EPC numbers of the products to be received and any available aggregation information. The goods are received at the agreed warehouse of R, equipped with an infrastructure of RFID readers. After the necessary authentications, all EPCs are read by R's capturing application. The EPC IS capturing application confirms the fulfilment of the business transaction to the ERP system and updates the EPC IS repository. A confirmation is also sent to company W stating that the transaction was completed successfully. Finally, the EPC DS is notified that new data is available about the EPC of P.

5.2.2. Misuse Cases

Figure 10 shows some security concerns and measurements that are derived from an inspection of possible misuse cases. An erroneous RFID reading process, due to possible mistakes or malicious intrusions, is one possible misuse case. As an additional security measure that can mitigate the threats of an erroneous read, the received EPCs are compared with the expected ones, including that of P. The EPCIS capturing application then only confirms the fulfilment of the business transaction and updates the EPCIS repository upon a successful comparison of EPCs. In addition to the internal verification of received EPCs, a secured reading process at the level of the RFID readers will also help mitigate the threats associated with erroneous reads.

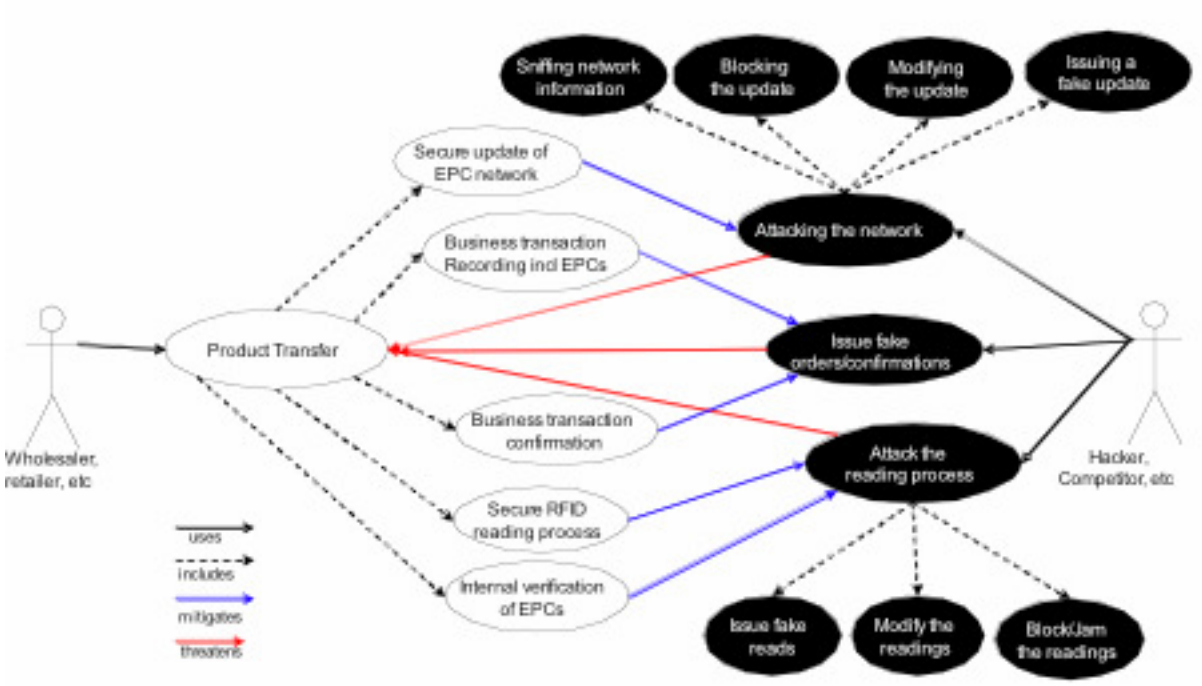
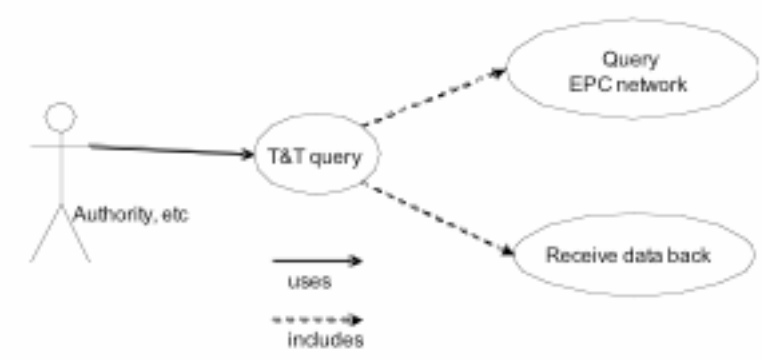


Figure 10 - Product Transfer Misuse Case Diagram

5.3. Track & Trace

Track & Trace (T&T) is the process of retrieving information about the movement and location of goods[7]. For a tagged product, a T&T query is expected to return the movement and location information pertaining to the queried product. Since the EPCDS, the network component which will make T&T possible, is still in the design phase, we don't know what functionality will a T&T service offer and thus what security concerns will it invoke. Thus we adopt a conservative approach in which the assumed functionality is the minimal one as defined by the EPCglobal network architecture specification [10]. Figure 11 shows the use-case diagram, followed by a narrative explanation of the scenario, and finally the misuse cases.

5.3.1. Scenario Description



[7] www.rfidjournal.com

Figure 11 - Track and Trace - Use Case Diagram

Authority A receives P and suspects that it was used in an illegal activity, so it requires authorization to T&T product P. Depending on A's access rights, proper credentials are provided to it by the industry's regulating body. Authority A uses the obtained credentials to authenticate itself to the T&T service. Upon authentication, the following steps happen in the EPCglobal network (as mentioned previously, this will be heavily determined by the EPCDS design which is work in progress – the steps below are merely an example):

- The T&T service queries the EPCDS to find all T&T information relating to P.
- The DS finds and returns the EPCIS references that store the relevant information.
- The T&T service queries (via the EPCIS query interface) the different repositories
- The data is returned to the service via the different query interfaces

The client application can further perform a plausibility check on the data, verifying for example that the product hasn't been at different places at the same time, etc., and then present that data to the user.

5.3.2. Misuse Cases

Figure 12 shows possible attacks that can jeopardize the results of a single query (like injecting false data) or the entire operation of the T&T service for some time (e.g. DoS attacks). Several counter measures can be envisioned to counter these security threats. Section 6.4 provides more explanations on the natures of the attacks and the possible counter measures.

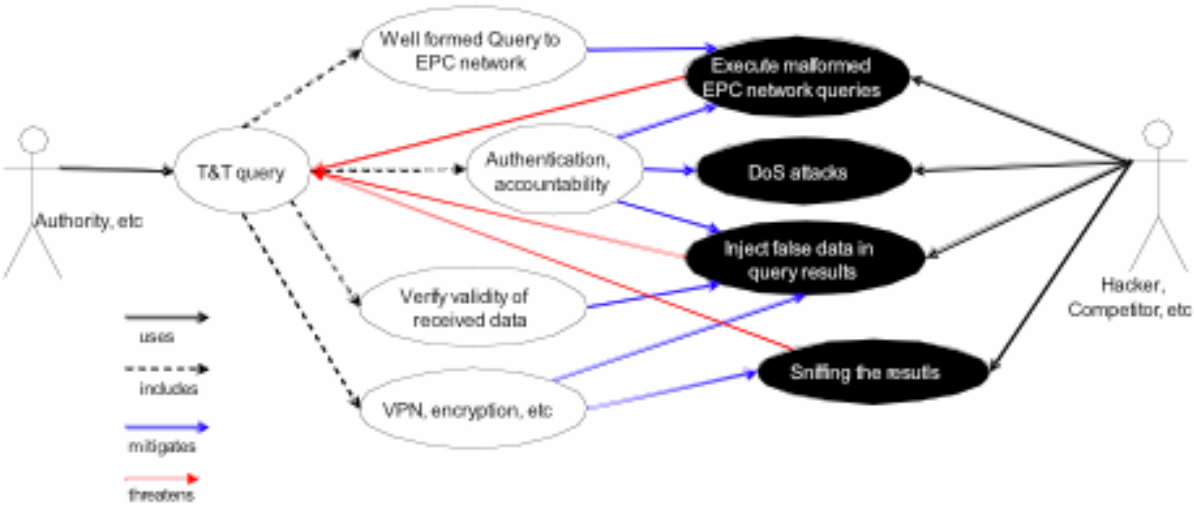


Figure 12 - Track and Trace - Misuse cases

5.4. Product Verification

The Product Verification scenario outlines how to authenticate a product with an attached RFID tag. Product authentication is an enabling application that secures the supply chain by preventing counterfeits. The application consists of two main use cases a) the direct authentication of a tag and b) the usage of serial-level information to reason about counterfeits. The assumption is that a licit actor L who wants to check the authenticity of a product P can access the track and trace records. Relevant serial-level events are those location events that relate to a shipping or receiving process. Figure 13 shows the use case diagram for the product authentication scenario. The following section will provide a narrative description of the scenario and then the misuse case diagram will be also presented.

5.4.1. Scenario Description

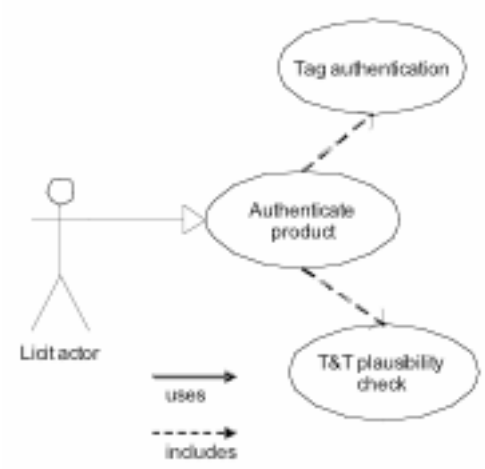


Figure 13 - Product Authentication - Use case diagram

Use-Case 1 Track and trace plausibility checks

Licit actor L wants to check the authenticity of product P. L sends a request to an anti-counterfeiting service A to carry out the plausibility check of P identified by its EPC number. A uses the Discovery Services to identify EPCIS repositories that have information about P. After gathering all parts of the track and trace history of P, the next check functions need to be addressed. It must be sure that the track and trace history starts at the manufacturer M and the origin is authentic. Additionally, it is required that the track and trace history is complete and provides a continuous flow from the origin at M to its last recorded location. For every part of the history, the origin and the truthfulness of the events are checked. The last known origin must be compared with the knowledge of L to ensure that also this endpoint is valid. At any point, A checks for anomalies in the track and trace record to find cloned products. These checks can include tests to ensure the singularity of the first event recorded by the manufacturer. Also more advanced checks that compare location and time data of events to find out whether a product movement was realistic or not are possible.

Use-Case 2 Tag authentication

Manufacturer M initializes the tag at her site and applies it to the product. The initialization involves an update of a backend database of an anti-counterfeiting service A. According to a secure authentication protocol, any licit actor L that possesses the product P can perform a tag to backend authentication that verifies the identity of the tag.

5.4.2. Misuse cases

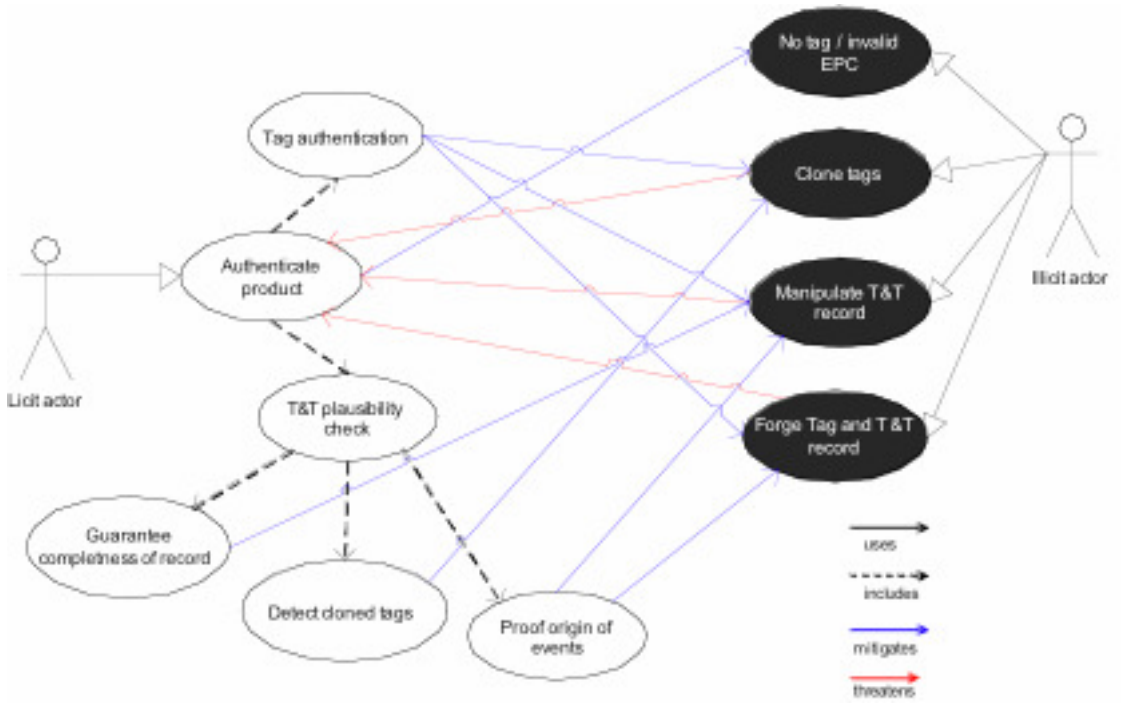


Figure 14 - Product Authentication - Misuse case diagram

5.5. Product Finalization

This section tackles the last phase of a product lifecycle whereby “kill the tag” is the main procedure required to protect consumer privacy. In order to provide a first approach, the simplest scenario will be considered: the tag is killed when the product is sold by the retailer to the final customer (e.g.: for confidentiality purposes). This general assumption is valid providing that the product sold has neither a warranty nor later support. In other words, once the product is sold and the tag is killed, it no longer exists for later initializations or movement events. In this way, tags that may be used to identify products which may be returned as defective or whose information may be required for recycling purposes are out of scope of this scenario. Furthermore, the next supply chains shall incorporate a new last recycling stage acting as a product end point and therefore the product lifecycle will be extended beyond the product sale. Despite earlier assumptions, the scenario shown below is illustrative enough to be considered valid in the present study. Figure 15 shows the use case diagram, followed by a narrative explanation of the scenario, and finally the misuse case diagram is depicted in Figure 16 .

5.5.1. Scenario Description

Figure 15 - Product Finalization Use Case Diagram

A product with an EPC code (assigned at manufacturing time) is sold by the retailer to the final customer. Just after the sale, the tag supporting the EPC code is killed and this operation is recorded in EPCIS and notified to the DS service through the EPC network.

5.5.2. Misuse Cases

Let us suppose that the tag of a product which is being sold (and therefore being killed) is counterfeited just before the sale by a malicious actor. Afterwards, the tag is killed and the notification is sent to the DS in order to update the corresponding databases. In the case that an event tries later to update the DS databases, we conclude that a cloning detection might have happened. Thus, because of the nature of the DS services, there are no additional needs to implement a security mechanism to prevent from “cloning” in this scenario.

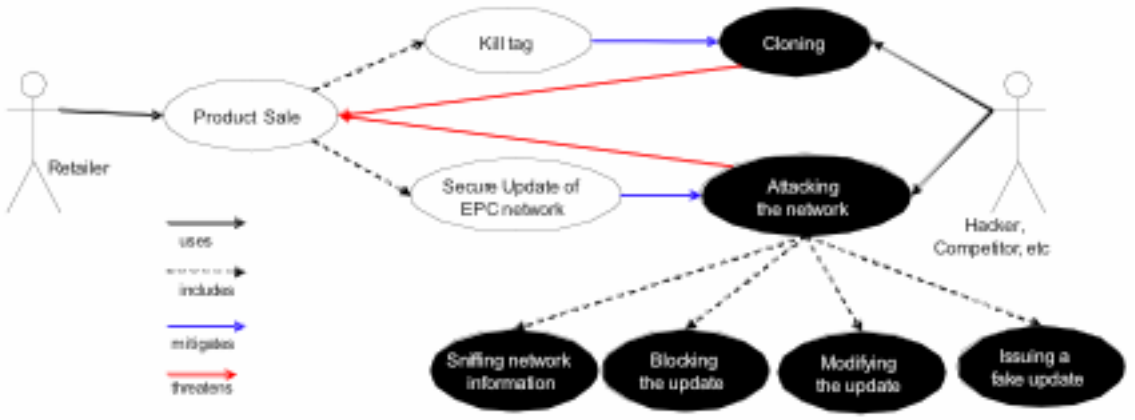


Figure 16 - Product Finalization Misuse Case Diagram

5.6. Conclusions / Findings

We presented in this section several scenarios that represent plausible usages of the extended EPC network infrastructure. The scenarios are the following:

- Product Manufacturing
- Ownership Transfer
- Track & Trace
- Product Verification
- Product Finalization

The above-listed scenarios were selected because of their representativeness and relevance for the upcoming infrastructure. They have a high probability of usage as they pertain either to typical supply chain operations (manufacturing, purchasing, and selling) or to other operations that support other work packages within BRIDGE (Track & Trace and Product verification). The scenarios and the findings were essential to highlight the extra threats associated with moving processes from the closed-loop to the open-loop infrastructure, which is along the same lines of focus of this report. They raise security awareness especially relating to the particular misuse cases that would only be possible as a result of the extended EPC network. Another merit of the selected set of scenarios is the fact that the requirements that can be elicited from the scenarios address the different layers of the infrastructure. This has the advantage of addressing different concerns simultaneously with minimal duplication of efforts and establishing a common language for the different subtasks to use and rely on. It should be noted however that the approach has certain limitations especially at this early stage of the infrastructure where in some cases the analysis and the threats can only be derived from generic specifications and not from finalized designs or existing implementations. One such example of crucial yet not completely defined components is the EPCDS, so detailed analysis is not possible at this stage. For such reasons, these scenarios will remain subject for modifications and additions even beyond this deliverable.
The considered scenarios were described and their security analyzed, and relevant threats were revealed. The threats span different layers of the architecture and certain countermeasures were recommended. The diagrams shown give an overview of the possible threats and respective measures needed to mitigate them. Some threats were common to different scenarios and the reader finds these duplicated in several scenarios to highlight their relevance and scope. One such example of attacks that are common to different scenarios is the set of attacks on the EPC network. Such attacks occur when a client needs to read in information available on network or update information there, typically residing on the EPCDS and/or EPCIS. The different attacks include sniffing the information being transferred, blocking the particular communication or even eventual communication (DoS attacks), modifying the information, and injecting false information. Other threatening misuse cases include cloning RFID tags, and attacking the read process in several ways: jamming the reads, modifying them, injecting fake reads, etc. In the next section we give more details about these threats and how they translate into security requirements on the different layers of the infrastructure.

6. Security Requirements of Different Layers

The BRIDGE project is an excellent opportunity to identify the security threats related to RFID technology and the EPCglobal network. The business work-package: WP5 Anti-counterfeiting, WP6 Drug Pedigree, WP7 SCM European Textile, WP8 Manufacturing, WP9 Asset Management, WP10 Product in Service and WP11 Non-food item-level tagging provide us access to pilot activities and end-user requirements that enable us to steer the focus of our activity.

Our objective is to address their security concerns with common security capabilities for the EPCglobal network that can enhance the value of these business propositions. To collect security requirements from the business pilots and other end-users we have performed interviews (Section 4) and we have also developed and discussed application scenarios to derive security concerns and requirements (Section 5). We have also held discussions with WP1 to address security challenges from a hardware point of view and WP2 to identify missing security capabilities in the EPCglobal network, and promote a secure design for an EPC Discovery Service.

For the purpose of requirements analysis we have divided the BRIDGE architecture into four different layers:

- Tag-layer security requirements that deal with the security at the hardware level in terms of physical protection for the tag and also in terms of protection of the information on the tag.
- Reader security requirements that are concerned with security mechanisms to protect the EPCglobal network from injection of malicious data or the compromising of confidential information.
- Network security requirements that address the security mechanisms necessary to design and operate a secure EPCDS (EPC Discovery Service) alongside other components such as the EPCIS.
- Application level security requirements that address the further security considerations of shared application intelligence and end-client applications.

Before discussing in depth the security requirements for each of these four different layers, we enumerate in section 6.1 all the security requirements that have been collected from the previous sections. We will then motivate a technical discussion around these points in the following sections of this document. The final objective is to map these early requirements with activities that will be addressed in the work activity of WP4 “Security”.

6.1. Summary of All Security Requirements from Previous Analyses

In this section we analyse the requirements for the layers of the BRIDGE architecture according to three categories:

- **Business Integrity**. These requirements deal with the integrity of RFID data and processes. It should not be possible to subvert or disrupt processes that operate using RFID data.
- **Business Intelligence**. These requirements deal with maintaining confidential business information. The owner of information should be defined and controls placed on the distribution of data to other parties. This category is also used to cover to sub-area of privacy where data collected by business processes may infringe personal privacy.
- **Operational and Deployment**. These security-related requirements cover the real-world deployment requirements of RFID systems including cost and inter-operation with existing technology and systems.

6.1.1. Business Integrity Requirements

Identifier	Layer	Requirement	Source
TI1	Tag layer	Tags should not be disabled when product is being used by business process	Interview. D4.1.1_Report_Security_Analysis Section 4.3.3
TI2	Tag layer	Tag must be secured against malicious writing of EPC	Use case scenario. Product manufacturi
TI3	Tag layer	Tag must resist movement between physical products	Use case scenario. Product manufacturi
TI4	Tag layer	Tag must have a unique EPC	Use case scenario. Product manufacturi
TI5	Tag layer	Tags must be verified after writing	Use case scenario. Product manufacturi
TI6	Tag layer	Tags must be authenticated	Use case scenario. Product verificatio
TI7	Tag layer	Cloning of tags must be prevented	Use case scenario. Product verificatio
TI8	Tag layer	Writing tag data must be protected when moving from closed to open loop	Interview. D4.1.1_Report_Security_Analysis Section 4.3.1
RI1	Reader layer	Companies internal systems must be protected from attacks by corrupted, malicious or fake readers	Interview. D4.1.1_Report_Security_Analysis Section 4.3.2
RI2	Reader layer	Injection of data from readers needs to be controlled in order to prevent the introduction of false information	Interview. D4.1.1_Report_Security_Analysis Section 4.3.4
RI3	Reader layer	Reader must read correct tags (without blocking, modification or introduction of tag information)	Use case scenario. Product transfer
NI1	Network layer	Architecture must be resilient to denial or failure of components	Interview. D4.1.1_Report_Security_Analysis Section 4.3.5
NI2	Network layer	The RFID infrastructure must allow effective anti-counterfeiting through multi-party track & trace information	Interview. D4.1.1_Report_Security_Analysis Section 4.3.7
NI3	Network layer	Origin of events must be provable	Use case scenario. Product verificatio
NI4	Network layer	Network must use secure updates to	Use case scenario. Product manufacturi

		prevent data corruption	
NI5	Network layer	Received data must be validated by trusted parties	Use case scenario. Track and trace
NI6	Network layer	Network transactions must be well formed	Use case scenario. Track and trace
NI7	Network layer	Network transactions must be authenticated	Use case scenario. Track and trace
NI8	Network layer	Transport security should be used to complement EPC network component security	Use case scenario. Track and trace
NI9	Network layer	There must be accountability for data validity	Use case scenario. Track and trace
AI1	Application layer	Product characteristics must be verified	Use case scenario. Product verificatio
AI2	Application layer	Tag movement between products should be detected	Use case scenario. Product verificatio
AI3	Application layer	Cloned tags must be detected	Use case scenario. Product verificatio
AI4	Application layer	The communicating partners should mutually authenticate themselves before a communications between companies	Use case scenario. Track and Trace
AI5	Application layer	A company may track and trace a product in order to verify its authenticity	Use case scenario. Product verificatio
AI6	Application layer	The system architecture must ensure that changes and access can be traced back to specific identities.	Interview. D4.1.1_Report_Security_Analysis Section 4.3.8
AI7	Application layer	EPCs must be recorded in business transactions	Use case scenario. Product transfer
AI8	Application layer	Business transactions must be validated and auditable	Use case scenario. Product transfer
AI9	Application layer	Completeness of records must be guaranteed	Use case scenario. Product verificatio

6.1.2. Business Intelligence Requirements

Identifier	Layer	Requirement	Source
TC1	Tag layer	Reading may be disabled when product is not within company influence	Interview. D4.1.1_Report_Security_Analysis Section 4.3.3
TC2	Tag layer	Readers must be authenticated by secure tags or transmit encrypted reply	Use case scenario. Product verificatio
TC3	Tag layer	After a product is sold to the final user the tag must be capable of being disabled	Use case scenario. Product verificatio
TC4	Tag layer	Reading tag data must be protected when moving from closed to open loop.	Interview. D4.1.1_Report_Security_Analysis Section 4.3.1
RC1	Reader layer	Corrupted readers should not be able to eavesdrop on tag events	Interview. D4.1.1_Report_Security_Analysis Section 4.3.2
RC2	Reader layer	Corrupted or fake readers should not be able to access internal business information	Interview. D4.1.1_Report_Security_Analysis Section 4.3.2
RC3	Reader layer	Reader should be authenticated by network components	Use case scenario. Product transfer
NC1	Network layer	Network must secure event collection	Use case scenario. Product manufactur
NC2	Network layer	Client queries must be authenticated and access control enforced	Use case scenario. Track and trace
NC3	Network layer	Companies should have choice on who to trust with hosted data	Use case scenario. Track and trace
NC4	Network layer	Companies should have control over hosted data (withdrawal & access)	Use case scenario. Track and trace
NC5	Network layer	Transport security should be used to	Use case scenario. Track and trace

		complement EPC network component security	
AC1	Application layer	The communicating partners should mutually authenticate themselves before a communications between companies	Use case scenario. Track and Trace
AC2	Application layer	Data must be transferred only with clear destination and usage	Interview. D4.1.1_Report_Security_Analysis Section 4.3.9

6.1.3. Operational and Deployment Requirements

Identifier	Layer	Requirement	Source
TO1	Tag layer	Secure tags should operate with existing insecure readers	Use case scenario. Track and trace
RO1	Reader layer	Secure reader should be able to operate with secure and insecure RFID tags	Interview. D4.1.1_Report_Security_Analy Section 4.3.1
RO2	Reader layer	A compromised reader should not provide means to attack other IT systems	Interview. D4.1.1_Report_Security_Analy Section 4.3.1
RO3	Reader layer	A reader should not allow injection attacks from malicious tag data	Interview. D4.1.1_Report_Security_Analy Section 4.3.1
NO1	Network layer	Network components should be resistant against Internet (Distributed) Denial of Service attacks	Use case scenario. Track and trace
NO2	Network layer	Network components should build upon existing standards and frameworks for identity and access control	Use case scenario. Track and trace

6.2. Tag-Layer Security

As we have discussed early in the document, current RFID Tag technology lacks the resources to perform cryptographic operations. Commercial tags have a couple of thousand gates to perform the basic operations. Thus, only few hundred gates are left to perform security functionalities. We have to agree with our interviewees that RFID tag security is still a long term goal. We also have to agree that given the choice of a cheap tag that costs few cents and a secure tag most end users will go for the cheapest solution.

However, we should not dismiss the need for security in the tag. As the number of RFID applications will increase toward open loop systems with access from many parties, we can foresee that the lack of security will be a big impediment in many solution designs. Our view is that Moore's Law and market drivers will soon enable security functionalities on low cost tags. The default choice of using cheap unsecured tags will change if tag security can be seen as a service enabler and we can make the security management easier and cheaper.

We shouldn’t forget that the security level for protection of a tag cannot be determined without any information about the final application. The tags are only one part of the overall system. E.g. car-immobilizers in combination with a key to unlock the ignition of a car, the security level is determined by the combination of the tag’s protection and the security given by the characteristics of the physical car-key. The value that can be gained by a successful

attack (hacking the tag and producing a copy of the key) is easy to assess and the security level of the tag and the key can be determined.

This approach prevents secure use of the same tags in other (or additional) applications. A serious incident that arose due to wrong application of security tags was published by a group of researchers of Johns Hopkins University in January 2005[8] . They hacked a contact-less payment system, based on tags originally used and designed for car-immobilizers. The tag's security requirements for a payment system that relies on the protection of the tags, is due to the possible fraud higher than for the car-immobilizer application. Many of the future applications of secure tags are not yet known; therefore we must avoid tailoring the security requirements for a specific application.

Future RFID systems are planned as open loop systems, with access for many different parties. Such systems must be built on standards easily accessible for any party. This accounts also for the protection mechanisms. Cryptographic primitives used for protection of tags should be available as open standards. During standardization of cryptographic algorithms, approval is only given after a broad public review process that should help to find weaknesses (e.g. the FIPS AES). Proprietary algorithms often lack in this sense, and therefore the algorithm itself is undisclosed to prevent successful attacks. Open loop systems prevent usage of undisclosed algorithms, since too many parties would need access to the undisclosed details and therefore disclosure of critical information would be very probable.

We therefore define the protection level for BRIDGE WP4 to use state-of-the art cryptographic primitives with appropriate key-lengths to prevent brute-force attacks. To allow design of open systems we rely on standardized algorithms with published specifications. As a reference we suggest to rely on algorithms used in smart cards for banking applications.

6.2.1. Business Integrity Requirements

Physical protection of a tag: Cryptographic tokens like smart cards or security USB tokens often contain a private key that is protected against read operations, but is only used for cryptographic operations. Tags with cryptographic capability will also store a secret key which must be protected. Smart cards and tags operate in similar environments, actually a completely untrusted environment, which means that the cryptographic device is under full control of the potential attacker. Attackers can easily get tags into their hands, they can try to operate them with their own reader, which means that an attacker can choose the operation and input data he provides to a tag. This makes attacks much more powerful than simply listening to a communication channel.

A very important fact is that attackers can use and destroy tags to get information about others. Since tags are available for a very cheap price in actually unlimited quantity, an attacker can operate tags of their specified range and try to find vulnerabilities under special circumstances.

[8] http://www.jhu.edu/news_info/news/home05/jan05/rfid.html

Smart cards are often protected by on-chip sensors to detect attacks which are performed during non-specified operation conditions (e.g. a clock-signal that glitches or reduced power supply, operation under high temperature). If a sensor detects a potential attack, the card refuses then further requests and stops operation. Due to the additional costs and rather high power consumption of such sensors this approach is not meaningful for high volume RFID tags, since they would raise the costs of a tag too much. The fact that a tag always operates in a rather strong EM-field (the carrier signal of the reader) is a drawback for the attacker. To operate the tag an attacker must provide the EM-field (and live with the high noise from the carrier) or dismantle the tag and remove the antenna from the silicon chip, to provide contact based signals without an antenna. Currently research is ongoing on passivation layers for the chips of RFID tags, which can be used to derive cryptographic keys [8] [9]. When the passivation layer is removed or broken by an intruder (to get access to the chip) the key is destroyed, and therefore the information stays protected. Research on this level is not a focus for BRIDGE WP4, but we follow the ongoing research activities and we will try to include recent findings into our proposals.

Side channel attacks (SCA) are a big topic in protection of security tokens like smart cards. When performing a side channel analysis an attacker uses not only input and output data to mount an attack, but additional side-channel information, like continuous power consumption during execution of a cryptographic algorithm (power analysis attacks) or simply the execution time (timing attacks). Those attacks turned out to be very effective and protection against this threat is rather complicated due to the high accuracy of available measurement equipment and the power of statistical tools. Within BRIDGE we will investigate this type of attacks to assess the vulnerability of cryptographically protected tags. Especially DEMA (Differential Electron-Magnetic Emanation Analysis) has to be investigated and if it turns out to be a realistic threat, protection solutions need to be proposed. The protection measures will be different from smart-card technology due to the very limited power budget available for operation of passive RFID tags.

6.2.2. Business Intelligence Requirements

Measures to protect information on the tag: Data on tags can be stored in encrypted form, meaning that a reader encrypts the data under a certain key before it is stored on the tag. An attacker cannot draw any conclusion about the meaning of the specific data without knowing the key, but in many scenarios this is not necessary to mount a successful attack. Tracking of tags is e.g. easily possible without knowing the “meaning” of the ID a tag broadcasts after every inventory request. Additionally it is easy to clone tags, since there is no need for understanding the semantics to produce an illegal copy of the data. Deeper investigation into this topic is not necessary to find out that this ad-hoc countermeasure does not provide sufficient protection.

To participate in challenge-response protocols for authentication or to verify a challenge a tag needs to be able to compute a cryptographic encryption primitive that involves a secret key. Therefore a tag also needs a protected memory to store this key. This memory must not be readable form outside, but is only used to store the key. As cryptographic primitives, block ciphers, hash algorithms or asymmetric cipher schemes are promising candidates to provide

the identified security operations. Some of the security operations additionally require a PRNG (pseudo random number generator) on the tag.

The acceptable additional costs for protection depend heavily on the application of the tags. There is a difference between tags that generate a product-identifier that links with information in the network (EPC vision-security requirements against tracking) and tags that can be used by specific applications as an additional memory attached to the product (security requirements for access control and authenticity of the information).

6.2.3. Operational and Deployment Requirements

Compatibility with non-secure RFID reader infrastructures: Secure tags must be still compatible with insecure readers. This means they must comply with EPC, but maybe with temporary IDs, or restrict access to some protected memory only to authenticated readers. This allows application of secure tags in standard supply chains, but makes secure operation (e.g. after POS) possible (think of personalized warranty of tagged goods – tags are readable only for the client and the merchant who sold the good).
Insecure tags must also be readable by secure readers. A security protocol should be implemented as a security layer above a standardized protocol to support this compatibility.

6.2.4. Required Security Operations of a Tag

During the requirement definition process the additional functionality of a tag was investigated. To protect the information stored on a tag or protect systems from clones or eavesdropping, different security operations need to be supported by the tag. Please note that not every application does require support of all possible operations:

- **Authentication**: (Tag authentication): The requirement for tag authentication comes typically from anti-counterfeiting applications. A tag that supports tag authentication can provide a proof of its identity by cryptographic measures. Authentication is furthermore necessary for applications that require anti-eavesdropping measures, since successful authentication is a prerequisite for encrypted communication.

- **Verification** (Reader authentication): Verification of a reader authentication is necessary for applications that need access restrictions to the tag's memory or functionality. To grant access for protected memory contents to a reader, the authentication of the reader needs to be verified before access can be granted or refused. Reader authentication is additionally a prerequisite for anti-eavesdropping protection for the communication between tag and reader.

- **Confidentiality** (Encryption): Encrypted communication between tag and reader is necessary for applications that need to prevent eavesdropping of the contact-less channel. Systems can be built in a way that tags operate only with encryption primitives (no implementation of the decryption necessary).

- **Signature**: RFID applications may require signature functionality for tags. With signature functionality a reader can request that a tag signs information sent to it. After signature a reader can prove that a specific tag has communicated with the reader. That scenario is interesting in applications with static tags (e.g. embedded into a billboard) that communicate with mobile readers (e.g. mobile phone with NFC interface).

6.2.5. Proposed Approach

Requirements for a BRIDGE tag prototype: Due to the limitations of budget planned for WP4 in general and the tag specific subtasks WP4.2 and 4.3 we do not consider producing silicon prototypes of tag hardware. To show that our approaches are feasible we rely on simulations of HW developments, which are accurate enough to prove that the given requirements for digital tag design can be met. To provide working prototypes we consider applications of programmable semi-passive prototypes, which implement the additional functionality on their firmware or on programmable hardware circuits (FPGA). This technology allows rapid prototyping for reasonable costs, but uses much more energy for execution compared to dedicated silicon prototype chips. The prototype tags for bridge WP4 will therefore have a back-up battery and come in a completely different shape, but provide the functionality of future passive RFID tags. The following list provides information about the prototype requirements we agreed on so far:

- **Semi-passive tag:** To save costs for production of silicon we will build our prototypes by using semi-passive RFID-tag platforms and extend them with security functionality. The semi-passive tags act as passive tags during communication with the reader
- **UHF Gen2 as protocol for prototype:** To allow development of prototype scenarios with reader prototypes (WP4.4) we decided to use the same protocol for the prototype tags.
- **Security operations as extension to UHF Gen2:** Security extensions will be accessible as security layer commands defined upon the Gen2 protocol layer. This approach guarantees downward compatibility to any Gen2 reader for the basic tag functionality.
- **Standardized crypto algorithms:** For protection we consider symmetric crypto primitives that are feasible for RFID tag implementations without reduction of the reading distance (less than 10µA power, less than 10kGates Area, approx 1000-2000 cycles). AES (Advanced Encryption Standard) is a very promising candidate, but Hash algorithms (SHA-1, SHA-256) are also under investigation.
- **Interfacing:** Additional to the air-interface, the prototypes will be equipped with a second interface (RS232 or USB, JTAG) as an additional communication possibility (e.g. for programming, debugging, testing or monitoring)
- **Programmable prototype:** The prototypes will be programmable via serial or JTAG interfaces to allow fast adaptation throughout the project.
- **Reading distance:** The prototypes serve as proof of concept for the developed protection methods, due to their semi-passive approach. Conclusion about the maximal

reading distance cannot be drawn, because this depends heavily on the final implementation on silicon. The reading distance for the prototype tags is therefore of minor interest.

6.2.6. Risk analysis for Research on Secure Tags

For low cost, high volume supply chain applications the costs for tags is absolutely crucial. If we fail to meet acceptable cost per tag, it is highly probable that the developed countermeasures are never applied.
On the other hand, the data protection laws regulate how information systems have to protect personal data. We must not ignore, that static ID numbers in combination with other data can be considered as personal information that needs to be protected against unauthorized use. Ignoring this fact can turn out to be a show-stopper for successful launch of RFID technology beyond POS terminals.
Standardization and compatibility needs to be addressed for all subsystems and therefore also for tags. RFID systems currently installed will be in operation for more than 2-3 years, therefore we need to make sure that our developed approaches are compatible to currently available technology.

6.3. Reader-Layer Security

Most current supply chain applications are closed loop within an integrated supply chain. They run in a tightly controlled environment without any special requirements for protection of the information. The tags themselves often sit within secure physical environments (e.g. warehouses) and the information is protected in part by the company's intranet/extranet. As we move towards collaborative or open loop supply chain scenarios the risks are higher since we start to deal with larger numbers of participants with varying levels of security and trust. We need to establish a way to measure and to manage these risks.

The reader is configured to collect information from tagged products and to inject this information into the supply chain network. We can consider the reader as a gateway that converts information from the physical world (zone of physical security) into the internal network of an organization (zone of information security). We can see that the reader needs to provide a controlled interface between these two worlds. For example, a reader should filter unwanted information or prevent malicious users from getting access to confidential information.

In line with the concerns expressed in section 4 and section 5, we have the following security risks associated with RFID systems, and in particular with the RFID reader:

- *Business Integrity Risks* - Injecting false tag information from an RFID reader could potentially disrupt the entire track and trace process. A direct attack on the reader could compromise the process that the reader was trying to enable.

- *Business Intelligence Risks* - A reader can collect confidential information for a particular business. It is important that this information is only shared with the appropriate organization and not with a potential competitor.

    - *Privacy Risks* - RFID technology could violate personal privacy and enable unwanted surveillance mechanisms. A reader is the first point of collection of this information. Again, it is important to manage how the collection is performed, to whom is the information passed, and for what purpose. Privacy can be considered as a special case of business intelligence where the information involved can be related to people.

- *Operational and Deployment Requirements* - A reader has to work with existing IT and network infrastructure and be managed as one part of a secure business. Computer network requires security on each single device to protect its integrity and its functions. The case of the reader is not an exception. We could imagine that an attacker can gain access to an organization's network by compromising a reader and by obtaining the valid credentials to access a network and attack other components. These attacks can compromise both business integrity and business intelligence.

In the following sections we outline these different threats in more detail, define a set of technical requirements for RFID security, and propose an approach that will be pursued within WP4-Security of BRIDGE.

6.3.1. Business Integrity Requirements

Process disruption was cited as the second highest security concern amongst the interview participants. The more specific threats of false information injection and the threat of counterfeit goods also ranked high amongst their concerns.

An RFID reader provides the ability to identify objects without line of sight. In certain cases this means that the system may be less resilient against a certain class of attack, since there is no visual corroboration of the presence of the tagged item.

For example, an attacker may be able to compromise a reader in such a way that when a tag is seen the reader transmits a different tag identifier. In this way an attacker can easily inject false information into the supply chain. This attack is similar to cloning the tag, but in this case the attacker does not have to program another tag to emulate the behaviour of the legitimate tag. Instead they attack the reader software.

Another attack with a similar objective is to impersonate a reader to inject spoof events into the supply chain. A distributed application for goods authentication requires multiple readers with different identities. The identity of the reader is used to infer business information about the tag reading event, such as "the product has arrived at the warehouse". The identity of the reader can be used to control what information a reader can introduce into the product pedigree. It is important to verify the identity of the reader before accepting information into the supply chain.

Factors that can influence the level of supply chain process risks:

- The existence of mechanisms or tools to detect false or altered information. For example: if the product Advanced Shipping Notice (ASN) has not yet arrived the product should not be within the organization.
- The environment in which the reader is located. If a reader is in a very controlled environment it should be harder for an attacker to compromise the software on the reader through direct access, or via an insecure local network. If a reader is in a remote or public environment without physical control then the risk is likely to be higher.
- The presence of security controls on the reader. If a reader provides a strong access control on the network interface, mechanisms to verify software integrity and mechanisms to authenticate the reader identity, then the risks can be reduced.

6.3.2. Business Intelligence Requirements

The interview participants ranked the disclosure of business information as the most significant threat introduced by open-loop RFID systems.

Collaborative ICT applications require the separation of the operation of the devices and networks from the control of services and content. This enables the operation of assured processes over a shared infrastructure.

We can imagine a supply chain application where a distributor provides a secure track and trace service for multiple organizations. In this case, the external entities may have access to their tag/product information directly at the reader level but they should not be able to gain any information about their competitor or adversary.

According to findings from the interviews, secure tags will not be accepted unless all members of the supply chain can understand the tags, and thus share the costs and extract value. A reader needs flexible support for security features, including the ability for local understanding of the tag without communication with external parties during the reading operation. This is essential to maintain high tag reading rates and ensure continued operation in event of network or system failure. In this case the reader requires a secret key to prove that it is authorized to read the tag or to understand the communication with the tag. If a reader is compromised and the corresponding secret keys are publicly disseminated, any protection for the secure tags will be lost. We need readers that can hold secrets securely, potentially even from the reader owner, and that communicate the reading data only to permitted and authenticated parties.

Factors that can influence the level of supply chain intelligence risks:

- The environment in which the reader is installed, and the sensitivity or value of the business information, are fundamental. If a reader is used in a “close loop” supply chain then access to the tags themselves or the information transmitted by the reader is reduced. However, we can imagine that as RFID technology proliferates and the value of the information that it carries increases, then these attacks will become inevitable.

- The availability of secure tags that can perform cryptographic algorithms. In this case, the tags would contain no more than an encrypted identifier and it could be extremely hard for an adversary to collect valuable information. However, in this case a mechanism to manage the tag secret must also be included in the reader.
- The use of authentication of the remote systems by the reader and the encryption of information transmitted by the reader over the network in accordance with permitted security policies.

6.3.2.1. Privacy Risks

In the last few years RFID technology has raised significant privacy concerns. Organizations that implement RFID solutions need to prevent the technology from infringing the privacy of the consumer. Experts participating in the interview process have identified that even if the real privacy threats of RFID technology are low, there is a significant risk that the perceived threats by end-users can lead to serious losses in company image and customer relations.

There is a risk that consumer organizations and media involvement can seriously hinder the willingness to use RFID in valuable areas. An organization could be held liable if it is found guilty of infringing current data protection regulations. The associated risk is that regulations could change and necessitate the change or withdrawal of RFID systems.

In order to safeguard consumer privacy we could include cryptographic algorithms in the tag. However, the main challenge is on the cost of such tags. Even without secure tags, an RFID reader could include mechanisms to enforce privacy policies. For example a privacy policy could say that if there is a “privacy bit” set on the tag, then we should not collect any information from it [1]. The technical challenge is how we enforce such a policy.

Factors that can influence the level of privacy risks:

- The proliferation of secure tags could prevent unauthorized users from collecting information without the correct secret key. Another factor is the presence of control mechanisms on the reader to enforce specific privacy policy, and securely operate tag decryption functions.
- The accordance with fair information practice principles to provide good notification and collect RFID information with consent and specified purpose.
- Legislation and data protection principles could play an important role in dictating the responsibility of companies in certain sectors (e.g. pharmaceutical, product authentication, etc.).

6.3.3. Operational and Deployment Requirements

An RFID reader is a networked computing device and therefore it can suffer from any networked attack, along with being a point of attack on other networked systems. We can imagine that an attacker that has compromised an RFID reader can get access to a company’s network and generate larger scale attacks. These attacks are not specific to an RFID solution but need to be mentioned to highlight potential future threats.

Specific attacks against an RFID reader can be a Denial of Service (DoS) that prevents communication with RFID-tagged objects. For example, an attacker can generate a jamming signal on the RFID spectrum. As has been observed from the interview results, the elimination of a single critical point of visibility in the supply chain can disrupt large-scale processes across many participants.

Recently a group of researchers at Vrije Universiteit Amsterdam discussed the injection of "malware" in RFID network [2]. When an RFID reader scans a tag, it expects to receive information in a predetermined format. An attacker could write modified data on a RFID tag. If the reader software has some security vulnerabilities (such as buffer overflow) then the malicious code could corrupt the process installed in the RFID reader, gain access to confidential supply chain information or mount attacks against other systems.

Factors that can influence the level of supply chain process risks:

- Integrity of the RFID software. If the reader provides strong access control mechanisms on the communication interface and the software (including the reader OS) is tested to avoid attacks such as buffer overflows and code insertion, then the risks of these attacks are limited.
- Other factors (as explained above) that can influence these risks could be the location of the reader, the level of network connectivity and the importance of the RFID application for a specific organization.

6.3.4. Technical Requirements for RFID Reader Security

In this section we derive a series of security mechanisms that could potentially mitigate the risks associated with an RFID system. We do not expect that these mechanisms are valid for all RFID applications. An organization would need to run a risk assessment analysis and cost performance evaluation to identify which security mechanisms should be deployed within a specific usage scenario.

Software Security and Integrity - The system owner and the application end user require that RFID readers conform to security and integrity expectations. The reader needs to implement access control on any interfaces that allow the modification of reader operation or access to internal information. The software also needs to be bug-free and analyzed to avoid security vulnerabilities that corrupt the operation or grant higher privileges than should be permitted.

Reader Authentication - We need to have mechanisms in place to authenticate the identity and the function of a specific reader. A rogue installed by attackers could impersonate a legitimate reader and make an organisation think that a process has been fulfilled when it was not.

Remote Integrity Check - The system owner and end users needs to have confidence and assurance of the RFID system. A remote attestation feature could enable any party to check that the reader runs a specific software build.

Support for Secure RFID Tags - The proliferation of secure RFID tags would require specific software components in the reader.

- Air Interface – Secure communication protocol. The reader needs to be able to identify in which way the information is encoded and implement different protocols simultaneously.
- Key Management – The reader needs to be able to identify which secret should be applied to encoded information. The right password or shared secret should be provided to the right reader with secure communication.
- Secure secret storage – The secret information required to decode the tag should be maintained in a secure memory part of the reader. A secret should not be disclosed to the wrong application, user or reader owner.

Policy Management - Provide a mechanism to guarantee that the RFID reader complies with a specific reading policy in support of fair information practice principles. A reader in the future may have to be compatible with data protection laws that regulate how the information should be collected when the reader is used in retail shop or in contact with consumers. Our interview experts were of the opinion that the most likely non-conformance to such practices related to the use of the data instead of the non-consensual capture, and the reader should support both principles.

Easily Managed - Where possible, a reader should provide a simple way to enhance RFID security without increasing the RFID tag and backend system costs. The Reader security should be managed as part of an overall company RFID security policy.

6.3.5. Proposal for a Secure RFID Reader

Currently supply chain applications do not make use of security mechanisms within the RFID reader. However, from our interview process and analysis of application security requirements we believe the need for an RFID reader with enhanced security functionality exists and will grow with time. The research activity in BRIDGE WP-4 task 4.4 is exploring ways to create a secure gateway to collect RFID information from the physical world. We will analyze the suggestion of Molnar, Soppera and Wagner [3] on the architecture of an RFID secure and trusted reader and we also plan to link our activity with the Open Trusted Computing (OpenTC) FP6 consortium [4]. OpenTC is focusing on the development of trusted and secure computing systems (embedded systems) based on open source software.

Our research activity is also inspired by the fact that trusted computing modules are becoming available on many computing devices. The objective is simple - if a device is trusted, then we can separate the operation of the device from the control of services and content. This enables the operation of assured multi-party processes over a shared infrastructure. This concept can be extended to allow control policies, secure secrets or processing modules to be installed and operated securely on the reader. A trusted reader

can operate in accordance with privacy consumer policies without raising tag production and management costs.

Within BRIDGE, we will explore the possibility to build a secure RFID reader product. CAEN RFID is planning to develop a secure RFID reader module that allows the installation and secure operation of processing components from privacy filters to decryption modules using an open service framework.

6.3.6. Risks for Secure RFID Reader Research

Security needs to be fit for purpose. Unfortunately since low-level infrastructure such as RFID readers may be used for many unforeseen applications, it is impossible to produce a single set of definitive security requirements. Thus any approach to reader security must allow flexibility in both tag and reader security capabilities. The reader must be able to be easily adapted to read secure tags without significant increased overheads. The reader itself also needs to support varied security functions such as access control on the reading and management interfaces, transport encryption, along with varied operational and auditing functions. These risks drive the selected approach within BRIDGE of building a multi-service reader.

Such a reader needs to be implemented with a low marginal cost above unsecured readers to ensure that it can be deployed in a wide range of applications that may require additional security at a later stage. If this margin is too high then unsecured readers will initially be deployed and re-used for applications where they introduce a significant weakness for attackers.

Security also needs to be managed, along with the routine operation of the reader. Any security features must not introduce vastly higher managed costs or expertise of operational staff. Complicated management processes can also introduce security risks themselves through lack of technical understanding, or social engineering.

6.4. Network access and enabling layer security

In this section we develop the threats and security requirements for the RFID Network layer of the BRIDGE architecture. The Network layer sits above the hardware of the RFID tags and readers, and supports business applications in their operations. Within BRIDGE we split the Network layer into the Local Network and the Global Network. The Local Network is comprised of components that are not shared between organisations. These components may be secured as part of a company's internal IT security. BRIDGE focuses on enabling global RFID solutions, and hence the security of the Global Network components is key to the collaboration between different companies handling RFID tagged goods. The security of the Global Network is about securing the high-availability components (such as the EPCIS, ONS and Discovery Services) that support *open supply chains*.

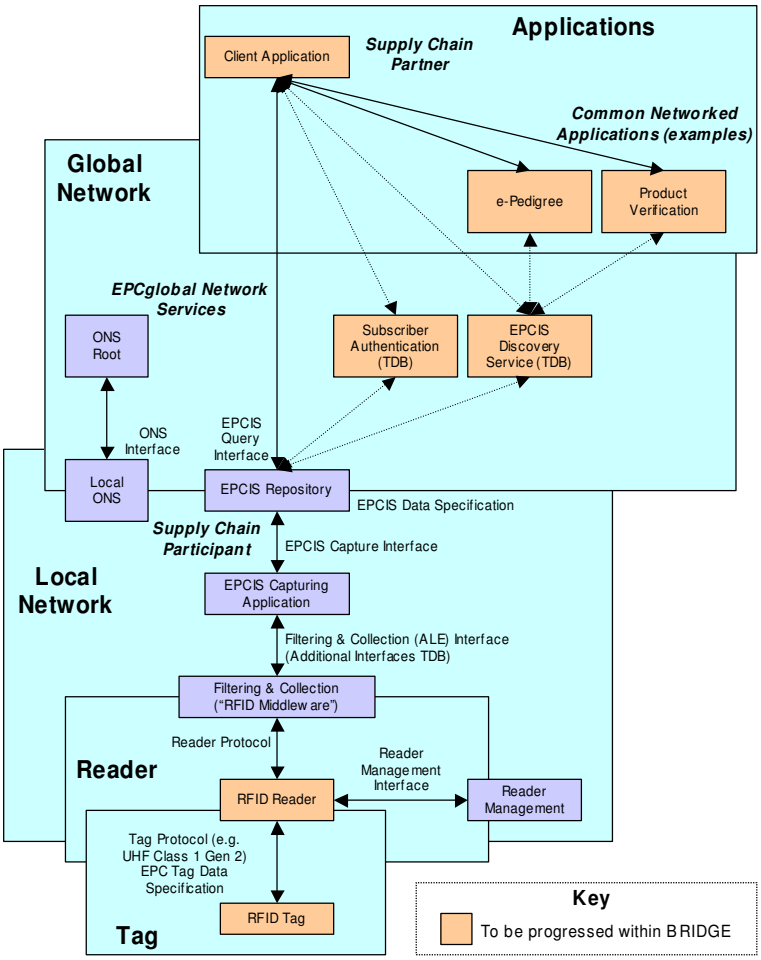


Figure 17 - EPCglobal Network Architecture

Note: Unlike other areas of the architecture, some of the Network layer components remain rather tentative and immature. Within BRIDGE we are involved in designing an EPC Discovery Service. In WP-4 we analyse the security considerations of design options for the Discovery Service and design the security extensions to enable a manageable, secure RFID network.

The basic EPCglobal network architecture exists fundamentally in order to support track and trace type applications between businesses. The objective of an EPCglobal network is to locate and retrieve information relating to objects carrying RFID tags with an electronic identifier (EPC). To locate EPC information from initially unknown parties, the architecture specifies two mechanisms: an Object Name Service (ONS) and an EPC Discovery Service (EPC-DS). In this section we look at security risks and implications for these components, along with the information repository (EPC-IS) of a single organisation. We then discuss in more detail the prototype implementation of the Discovery Service developed within WP2 of BRIDGE, and the security requirements of this globally networked component.

Note: networking elements are also present within a single company domain (notably the ALE/event middleware and the RFID event capturing application), but these exist within an

internal 'intranet' environment for which security practices are already well established. Hence our focus is on the external, 'open', shared network infrastructure.

Securing the Network layer components of the EPCglobal architecture represents perhaps the greatest security challenge. These parts of the infrastructure are common to a huge range of applications and industry sectors. Hence the impact of any security breaches (or erroneous operations) is likely to be of great significance. In line with the concerns expressed in section 4 and section 5, we have analyzed the security risks in the following areas:

- *Business Integrity Requirements* - Injecting false information into a network could potentially disrupt the entire track and trace process and applications that build upon the base of Network components. We need to control who can load information into the network, and maintain a provenance of such information to make informed business decisions. We need mechanisms to check that information is valid, accurate and up-to-date. In addition we need to ensure that such network components are not subject to availability attacks, or facilitate such attacks on other parts of the global RFID system.

- *Business Intelligence Requirements* - Disclosure of information collected and stored in the EPC network should be controlled. Even if we ensure that the information in the EPC-IS is secure, we also need to ensure initial ONS or EPC Discovery Service communication remains confidential. In addition to the confidentiality of the publisher of the information, we also need to consider the confidentiality of the client application who is using the Network components to retrieve information.

    - *Privacy Risks* - An architecture to enable global Trace & Trace applications could violate personal privacy and create unwanted surveillance mechanisms. It is important to manage the disclosure of the personal information in accordance with fair practice principles, and to consider how information might be linked to individuals.

- *Operational and Deployment Requirements* - It is important to consider that the Network layer RFID components will not work in isolation. They will form part of an economy of global services that includes many other non-RFID systems. It should be easy to develop a client application to engage with both RFID and non-RFID services. Similarly, security should be managed across all services and information exposed by a company – not just the RFID Network.

6.4.1. Business Integrity Requirements

Data Integrity – This requirement refers to validity of data information contained in the EPCglobal network. This covers both the correctness and completeness of the information, since the blocking or removal of key information could disrupt business operations along with the more obvious risks of data manipulation. It also involves the timeliness of the information since delays in state changes can lead to the subversion of the business operations. For example, the reference to an EPCIS in return of a specific EPC Discovery Service query should be correct and no adversary should be able to compromise this information. It is

important that this EPCIS record is up to date. These requirements will grow in importance as more critical business decisions are based upon RFID data.

We can draw a parallel with the Internet in order to describe the impact of security vulnerabilities for the EPC Discovery Service and the EPC ONS. Considering the vulnerabilities of the DNS (Domain Name Service), IETF RFC 3833 (reference) provides an excellent summary of the vulnerabilities of this system. Attacking the DNS is an effective method to corrupt the integrity of Internet based applications and services. A corrupted DNS could direct applications to communicate unknowingly with a malicious server. The DNS is a query –response application and a critical security feature would be a mechanism to provide authentication of the response provided by the DNS, along with authentication of any updates to the DNS records. The security requirements for a secure DNS service have been captured by DNSSec[9].

If an attacker is able to launch a successful attack on an EPCDS, the attacker could introduce a list of invalid EPCIS interfaces. If the there are not sufficient security measures at the EPCIS level, the attacker could inject false information into the system and potentially corrupt track and trace information. Even with controls that allow the authentication of valid EPCIS repositories, client confidentiality can be compromised and processes hindered as they attempt to identify legitimate systems.

There are several requirements relating to data integrity:

That the data provided is accurate. The threat here is that parties may maliciously inject inaccurate or disruptive information into the system (or conversely, they may fail to appropriately inject necessary information). Potential attacks include:

- **Record poisoning -** Attacks can change or manipulate the record held by the EPCDS or ONS.
- **Impersonation attacks -** Attackers may be able to impersonate a legitimate EPCDS or ONS and respond with fake messages to authentic queries.
- **Manipulation of communications -** Man-in-the middle attacks to corrupt information.

Potential solutions include a mix of technology and regulatory enforcement. We need to define mechanisms for RFID network components to validate the authenticity of any information update. We also need authentication on responses from EPC components to application clients. This includes authentication of the component itself, such as the Discovery Service, along with authentication of the provenance of the data returned. Each client should be able to assess the data integrity and the validity of the response. The EPC Discovery Service or ONS query-response protocol should be secured and the communicating parties should be able to detect any anomalies in the information.

In order to provide data integrity features for a query-response protocol, we can use digital signatures based on public key cryptography. Public key cryptography relies on the assumption that if client or service private key is kept confidential then we can setup a secure

[9] http://tools.ietf.org/html/rfc4033

communication. However, in order to be confident about this assumption we have to rely on trusted third parties (i.e. Authentication Service) that can create chains of trust. These parties are known as “public key infrastructure” or PKI. The establishment of this federated PKI is one of the main challenges that needs to be solved in the development of collaborative web-services. A possible approach for BRIDGE and for the EPCDS implementation would be to build upon such general PKI capabilities, using the Liberty Alliance approach to create a secure federation of EPCglobal services.

That parties are held accountable for their contributions to the system. Data published in the EPC network can be signed so that individual parties can in principle be held accountable for the quality of the data they provide. Again we could use public key cryptography to achieve this goal. Contracts and legislation may mandate what data must be provided, and the timeliness of the data provision.

Public key cryptography can also provide the property of non-repudiation. Non-repudiation is defined as the inability of a person to deny having made a digital signature. However, relying on electronic non-repudiation may contradict some legal practices. Along with preventing the ability to deny a signature, we also require that the information bearing the signature may not be withdrawn. Network components acting as Trusted Third Parties may provide such undeniable logs.

In order to help ensure that only accurate data is recorded in a company’s EPCIS repository and directory services such the Discovery Service and the ONS, we could require that these RFID systems be audited regularly. Regular audit procedures should be in place across companies that are willing to collaborate in order to guarantee that data information is complete and up to date and to improve trust across the overall architecture.

6.4.2. Business Intelligence requirements

Confidentiality - There are many scenarios where the information held within an RFID network could be regarded as sensitive information. This can include information revealed by a client application during an EPC search operation, along with information published into the network through the EPCIS interface and Discovery Services. Open loop supply chains where different players have global visibility of the assets throughout the supply chain require careful attention to security. In these cases we have to make sure that supply chain players do not receive information about competitors that use the same RFID infrastructure.

The problem is complex. Depending on the application scenario various categories of problems could be defined.

- When a supply chain application queries an EPC Discovery Service or ONS, the application would have to agree to disclose his interest *(e.g. “I am interested on EPC: x.y.z.*”)* to RFID network. A malicious EPC Discovery Service could use this information to profile the supply chain service client.

- At the same time an EPCIS that publishes information to an EPCDS would require that the information is only disclosed from the EPC Discovery Service to selected parties.

Again a malicious EPC Discovery Service could use this information to profile the EPCIS or leak confidential supply chain information.

- The EPC Discovery Service and EPC ONS will receive queries from hitherto unknown players. We need a mechanism to identify and authenticate the different players. The EPC Discovery Service will also require mechanisms to control which information should be disclosed to which players.

- External adversaries can monitor the traffic received by the EPC Discovery Service or ONS. In most applications we would require confidentiality on the message exchange between the different parties.

In BRIDGE we initially assume that the client application and publisher of information can find a mutually trusted Discovery Service, ONS and PKI infrastructure. During the second part of the BRIDGE activity we will challenge this assumption. However, in our support of WP2 in designing a secure Discovery Service this assumption appears to meet the current requirements. Working without a trusted Discovery Service would require schemes that exploit cryptographic algorithms such as being able to operate encrypted searches over encrypted data.

We can define a number of requirements relating to confidentiality:

The data communication is confidential. There is a requirement that data provided to the network components such as the EPC Discovery Service is transmitted and maintained without access to unauthorised parties. Data transmission should only occur after the receiver is authenticated and should employ encryption to prevent eavesdropping.

This requirement can be met through the standard secure transport mechanisms such as SSL or HTTPS. It should be noted that even when employing transport encryption the identity of the party is revealed. Thus, although a client application's interest in certain EPC numbers may be secured, the fact that it is communicating with the Discovery Service may not be.

That exchange of data is controlled between authenticated parties. A critical element for an EPCglobal network is access control. The objective is to limit the ability of parties to publish or receive information. Information should only be disclosed to authenticated parties based on predetermined rules.

The problem of properly controlling access to data is known to be difficult. Strict control of access is quite simple in principle, but the manageability problems grow as the systems become more distributed. An access control model must ensure that the injection of false information is prevented but it also has to selectively control the release of the data. The complexity of access control grows in an open loop supply chain since the product flows along a path that cannot be predetermined. It is also expected that the data released to different authenticated identities will vary to meet the demands of different applications.

The main requirements in terms of access control are:

Access control management service and security policies. This service should be part of the RFID network architecture and provide mechanisms for organizations to define access rules for specific data records. This service should be able to associate a specific identity (e.g. organization or application), along with roles and other resource access credentials. These rules or policies should be cohesive, but distributed across the RFID network to allow local enforcement. We expect to use standard security policy languages where possible such as eXtensible Access Control Markup Language (XACML).

Authentication service and resource access credentials. There is a requirement for the communication protocol to carry information about identities and roles. For example, an EPC Discovery Service or ONS query about a specific EPC record should carry information that allows the network component to identify (authenticate) the client and make a decision in terms of disclosure. Where communication is relayed between network components, such credentials and other assertions must also be relayed. We expect to use a specification language that is sufficiently rich to capture the full range of control features (e.g. Security Assertion Markup Language (SAML)). One or more Authentication Services using a federated PKI may generate these credentials.

It should be noted that in BRIDGE, WP-4 expects to suggest an appropriate access control solution for the EPC Discovery Service and EPC ONS. However, this solution will not be an innovative bespoke solution but it will be compatible with existing W3C and OASIS standards. It should be able to accommodate multiple authentication and key management services. The innovative research will be focused on how to manage the scalable definition of access control across open supply chains.

Prevention of data-mining. This risk will become a growing threat in open-loop supply chain applications. Commercial parties are very protective of the confidentiality of their business and will only engage in a RFID network if they can be assured that data mining is minimized. Even when access control and encryption are in place, data mining attacks can still compromise confidentiality. For example, an adversary could learn that a certain pattern of communications indicates that a pallet has arrived at a distributor from a certain manufacturer.

These attacks are facilitated when the identity of the communicating party is visible. We should also be aware that a party not intending to disclose their identity might still be identified by information such as network addresses or network location.

Prevention of data mining it is a challenging task. The approach is to prevent the discrete observation of RFID based events and communications. Secure networks such as Virtual Private Networks (VPNs) do not provide an answer since we must assume that attackers are inside the network (since they may be legitimate participants in the supply chain). There are a couple of options:

- Outsourcing (hosting) information from multiple sources onto a shared trusted repository could enable queries to be handled without onward communication that may

be analyzed. Such an approach requires trust in the shared resource and exposes significant risks should the trusted party be compromised.

- Running sensitive EPC services (EPC Discovery Service, ONS and EPCIS) over an anonymous mix-net [30], can hide identities and distribute communications over alternate network paths. The disclosure of identity and credentials for access control would only happen during a mutual authentication process. In this case we would maintain a completely private RFID network architecture.

6.4.3. Operational and Deployment Requirements

RFID network components such as the Discovery Service are available over a shared network that exposes them to the effects of network attacks. Furthermore in many cases we expect these components to be globally reachable from the Internet and not hosted on a secure private network. Such components are also built using commonly available Operating Systems and middleware (e.g. Application Servers). Thus they are also subject to vulnerabilities in these supporting systems.

A major security issue for shared services such as the Discovery Service or ONS is service availability. In particular if you consider EPC services that are vital for supply chain processes (e.g. “pharma ePedigree” or “product-authentication”) we should be able to guarantee a minimal amount of service downtime due to security vulnerabilities and attacks. Networked services should be protected by classic security mechanisms such as firewalls and IDS (Intrusion Detection Systems). Denial of Service attacks can take several forms such as network bandwidth attacks, along with attacks that overwhelm the processing capability of the component itself. Designs that maintain state during distributed transactions are more vulnerable to this latter type of attack.

Distributed Denial of Service (DDoS) attacks are a significant problem since it is hard to distinguish legitimate clients from the attack itself. To protect against these attacks we require replication and distribution of the RFID network components over different locations in the network. We need to avoid that our infrastructure has a single point of failure that is exposed to the attacker.

6.4.4. Proposed Approach

The objective of this section is to introduce the set of high-level security requirements that apply to the design of the Discovery Service (DS) prototype to be developed in WP2.

The Discovery Service prototype must be built using system engineering principles according to [27] in order to cope with the characteristics of distributed system processing: remoteness, concurrency, lack of global state, heterogeneity, autonomy, evolution, and mobility. In order to deal with these characteristics, WP2 aims to enable the building of a Discovery Service with the following properties: openness, integration, flexibility, federation, modularity, manageability and security.

The security characteristics of the Discovery Service are controlled by high-level security policies. Security policies define the rules by which the DS governs access to its resources: information records and discovery capabilities. The behaviour of the system derives from the combination of these security policies along with the design of secure components. The security characteristics of these components are developed from the requirements of the applications and the threats within the operating environment.

Before seeking security requirements, the first phase is to determine the objects of the Discovery Service requiring protection to which security requirements or policies will apply. Discovery Service records are the main asset that is stored and exchanged between parties. In addition to the information records, the identity of the parties that request or update Discovery Service records form another asset that must be protected.

The high-level security requirements [28] enable the Discovery Service to protect the assets and to enforce the established security policies. The requirements stated below are descriptive, while the detailed formalised security requirements are omitted from this document.

Access Control. Control of the disclosure of data is an important security objective. Access control must provide a mechanism to limit the access to the resources: queries or updates. Authentication mechanisms must be used to establish the relationship between the client and the resource.

Data Confidentiality. Communication between the publisher and the EPC Discovery Service or between a Track and Trace application and the Discovery Service should be secure. Interfaces should assure confidentiality in the exchange of data.

Data Integrity. External transactions between external parties and the EPC Discovery Service should have data integrity implemented according to the particular organisational security policies. Authentication of the data and the identity information could be provided through public-key cryptography. In certain applications we could also consider mandatory the non-repudiation of the origin of the data. Assurance of the integrity of the data received can also protect against injection attacks or exploitation of vulnerabilities such as buffer overflow attacks.

Secure Audit. Information related to security relevant activities should be recognised, stored, and analysed by means of a secure audit.

Guaranteed Service Availability. Attacks on processing capabilities, storage capabilities and network bandwidth could undermine the availability of the service. We need mechanisms to provide priorities among users (e.g., updates over queries) and preventing users from monopolising resources.

Authentication and Access Control Management Services. A working implementation should provide supporting services to manage access credentials and define policies. A possible approach is to use federated authentication/identity services such as Liberty Alliance.

Finally, additional security requirements that must be considered are: limitation on multiple current sessions, trusted disaster recovery, replay detection, reliable time stamps in DS records, expiration of state (at certain point in time) and revocation (at some point in time) rules and security management roles.

6.4.5. Risks for Secure RFID Network Research

The risk of providing inadequate security for networked RFID components within a company is that security will be bolstered by a variety of proprietary developments. The risk of providing inadequate security for the globally networked components such as the EPCIS and Discovery Service is far higher. Proprietary security for these components will lead to a proliferation of expensive bilateral arrangements and localised secure networks. The cost of developing and maintaining these arrangements will hinder their formation. Furthermore the fragmented approach will lead to businesses being unable to extract value from the distributed information, and hinder the formation of dynamic business arrangements. Such fragmented approaches can also lead to unknown security interactions and the inability to understand the overall security policy and operations of a company. The ultimate outcome is that companies will be unwilling to co-operate and that the vision of global RFID enabled processes will never become reality.

The deployment and operation of secure systems must also be economically viable. This means that the cost of the systems themselves must not be increased significantly, but also that the staff required to deploy and manage such systems must not require vastly higher levels of effort or expertise. For these reasons, RFID security should not be developed in isolation from other globally networked IT systems. RFID components should inter-work with non-RFID systems. In this manner they can share development and deployment costs and re-use expertise. The use of wider standards also builds confidence in the security of such solutions and their future evolution.

6.5. Application-Layer Security Requirements

6.5.1. Introduction

For the extended EPC network infrastructure to be widely adopted, applications should be found that make a profitable case out of using it. Example applications that will be investigated within BRIDGE include Track & Trace, Product Verification and ePedigree. Such applications are either entirely new or will be operated under different conditions than before. This will force us to look at security-related concerns from a new perspective, taking into consideration the concerns of the businesses that would use the proposed applications. We will have to investigate scenarios in which adversaries or competitors can use the technology or the infrastructure to gain unauthorized knowledge. One such scenario is, using a hidden RFID reader, to physically scan the items at a competitor’s retail shop. Repetitive similar scans would enable the competitor to monitor the retailer’s business activities. Other scenarios we have to investigate are ones in which the vast amount of available supply chain data and its fine granularity might render the current security measures obsolete. If we don’t

target scalability issues beforehand, we might end up with situations equivalent to DoS attacks.

6.5.2. Business Integrity Requirements

Business integrity requirements stem from the need that business processes are not hindered or negatively impacted in any way as a result of using the proposed applications. The ultimate goal of businesses is that their processes are enhanced and the ultimate threat is that the processes get delayed, interrupted, or even totally cancelled because of the new infrastructure. Following are examples of business integrity requirements.

Non-intrusiveness: The applications must not intrude the usual business activities for (security) reasons that don't add any business value. For example, it is unreasonable to expect an employee to authenticate herself manually to numerous other players in the supply chain before each Track & Trace query. Authentication by different employees into other companies' information systems should be as transparent as possible without jeopardizing security.

Regulatory compliance: In some industries there are strict regulations that companies should adhere to, and those include security regulations. It is essential for companies to adopt systems that comply with the regulations in their respective industry. This makes certain applications require specific security related measures that others don't. A typical industry in which regulatory compliance is a must is the pharmaceutical industry, so this requirement is particularly relevant for the ePedigree application.

Uninterrupted availability of internal processes: An application that uses Track & Trace capabilities assumes that companies will have some sorts of databases (presumably the EPCIS) open for querying. Despite the abundance of the incoming queries, the company-internal processes shouldn't be affected or halted. For businesses, the availability of their internal processes is more crucial that replying to queries that provide added values to the community, even maybe to their competitors. Technically, this may or may not force a decoupling of the company's EPCIS and its ERP systems. The decoupling would support the unaffected availability of internal processes whereas the coupling may imply the undesired replication of vast amounts of data.

6.5.3. Business Intelligence Requirements

Disclosure of confidential information was listed as the most relevant security concern and was given top priority by the interviewees. We point out here the requirements that cover business intelligence topics such as data protection, privacy, and trust.

Data Protection and Privacy: Data that will be potentially shared in the future systems due to the increased supply chain visibility will probably be humongous. Such data will be only shared among companies if there are measures that insure the protection of the data and its integrity against malicious or inadvertent modification. In addition, the privacy concerns of companies and customers should be addressed, otherwise the companies won't commit

easily to sharing their data and compromising their customer relationships. Some of the guidelines relating to data acquisition are the following:

- Data collected should be adequate, relevant, and not excessive.
- Data should not be kept longer that necessary.
- Companies and customers have the right to know which data, about them or their products, is stored.
- Data collected should be processed for a specific purpose (e.g. data mining to infer new, unauthorized data shouldn't be permitted or feasible).

Trust: In business contexts, trust is a very delicate matter that goes hand in hand with authorization and access control. It is very hard for businesses to trust foreign entities, whether they are individuals, organizations, or applications. If a new security model is being proposed in the context of the new infrastructure and its example applications, it shouldn't imply that businesses relinquish control of whatever they perceive as their's. If this is a must, companies should be consulted and they should be assured that their concerns are met with the proposed trust model.

6.5.4. Operational and Deployment Requirements

Interoperability: Any new security mechanisms and trust models may have to affect the in-place mechanisms and the current applications. Interoperability is a must since a complete migration of the currently used mechanisms into a newer model would imply high costs. Interoperability is not only an intra-organizational requirement but should be observed between different corporations. Companies will likely pass through a transition period in which their and their partners' applications use a mixture of old and new security mechanisms so co-existence for a period of time is a must.

6.5.5. Security Technical Requirements

Roles and authorizations: Access rights are typically accumulated into roles and distributed to employees in a company depending on the level of access provided by their roles. Depending on the role an employee has, she will have different access rights. These rights are checked when the user is being authenticated, for example before performing a transaction with a certain partner company. In the current situation, security measures and checks are usually executed on a company-to-company basis prior to the communication, in the sense that any communication usually involves only a pair of trading companies and measures are in place to insure that this communication is secured. In the upcoming open-loop supply chain, we expect that companies interact with each other in a much more complex way than in the current case. A single employee can with a single operation indirectly require information from several companies and start a transaction that is propagated into many partners. Some of these partners may be previously unknown to the company requesting the communication or there has been no previous contract that regulates access issues between the companies. The role and authentication concepts being used in the current model will have to be adapted or reengineered to match the needs of the upcoming model, above all scalability. New or adapted ways are needed to achieve trust

between trading partners who don't know each other a priori. The solutions we develop should honour the business requirements mentioned above, including the non-intrusiveness requirement. It may be unrealistic to require new credentials for each employee of a company when she is about to perform a query or transaction that involves a new supply chain partner.

Auditing: An auditing capability should be provided by the system to provide accountability if and when something goes wrong. With an auditing mechanism, events can be tracked and the person responsible identified, thus a series of events can be reconstructed at a later date, allowing us to prove who was responsible for which events. Auditing is already provided for closed loop systems, so the difference we expect in the open-loop scenario is an extended auditing with the possibility/need of including extra-company players and auditing their actions in case they jeopardize the company data. This will depend on the expected architecture and how open it is.

6.5.6. Proposed Approach (for BRIDGE prototype)

Authentication and Authorization: As already stressed, authentication and authorization should be emphasized in the proposed applications and a scalable, non-intrusive model should be selected. We described in the previous section the as-is situation and expressed our concern that this might not be adequate, especially when a communication can include several parties simultaneously. We will investigate the possibility of using public and private key authentication as already proposed in other pervasive computing environments [15, 16]. The use of cryptography is widely acknowledged to secure distributed and pervasive systems [17] but the actual implementations are scarce for several reasons, most importantly the perceived reliance on a central, trusted certification authority (CA). The problem is that corporations want to be under control and one CA that many parties can trust is hard to achieve. Some promising works [17, 18, and 19] question the need of a central CA and propose mechanisms in which parties can exchange keys and authenticate themselves in distributed and pervasive environments. We will investigate the applicability of these security mechanisms for the EPC infrastructure applications and decide on the optimal authentication strategy that will satisfy the practical needs of businesses.

Revisiting current access control mechanisms: As pointed out earlier, the vast amount of data, its fine granularity, and the envisioned "openness" of the extended EPC infrastructure are all reasons to rethink the current access control mechanisms. The typically used access control mechanisms rely on the traditional Role Based Access Control (RBAC) mechanisms [11, 12]. Despite their simplicity, RBAC may not be the optimal solution we require for access control in the proposed applications. This is due to their inherent problems and to the additional requirements of these applications. RBAC focuses on the subject – on the entity that requires accessing an object. In the envisioned infrastructure, more emphasis will be put on the actual items whose information is to be accessed (due to item-level accessibility) and to the location (thus the owner) of the items. Such reasons make us investigate more general access control mechanisms such as the Generalized Role-Based Access Control model (GRBAC) [13, 14] which allows a policy to be based on the subject, object, environment, or any combination of these. Another challenge is specifying access control on the fine-granular item level to external entities that we probably don't even know of. Two aspects are worth

investigating here: (1) Automated Trust Negotiation (ATN) [31, 32, 33, 34, 35, 36] and similar mechanisms that determine the level of trust of external entities with minimal human intervention and (2) automatically specifying the access rights on data objects depending on their importance, location, and other context information [20, 21].

6.5.7. Risks

Since the infrastructure and the applications that will use it are still work in progress, it is difficult to describe the most pertinent security concerns that these applications pose, let alone name the risks that their implementation faces. However, from the points discussed in this section, a few challenges are the most relevant. A situation might arise in which the proposed applications would not work as required except if companies, say,

- relinquish control of their data and conduct transparent operations that contradict their business interests, or
- face halting operations because of lack of interoperability or process availability problems, or
- have to trust entities that they would have otherwise regarded as us trustworthy.

The security mechanisms should be built in ways to avoid running into such risks that are not affordable by businesses.

6.6. Scope of WP4 Tasks for Security of BRIDGE

In the previous section we have captured the requirements on different layers in the BRIDGE architecture from the interview and scenario analysis activity. We have arranged these requirements into three categories: business integrity; business intelligence; operational and deployment. These requirements have been used to discuss each architecture layer in turn, discussing these findings and deriving technical requirements and potential solutions that will be pursued within WP4 during the remaining BRIDGE project. The resulting list of requirements is presented in Appendix A, according to security taxonomy.

In the following section, we describe how the future technical work in WP4 will seek to address the requirements identified in this report. We have developed the requirements from both RFID users and what we consider to be realistic future RFID scenarios. Since security measures add significant costs to a system, the open market typically does not call for countermeasures before there have been successful attacks resulting in significant loss. However, in the case of collaborative RFID supply chains we believe that such systems will not develop initially unless there is adequate security. Furthermore we think that it is necessary to develop solutions against possible attacks, so that implementations are available when called for. We also need to ensure that current developments and standardisation activities do not progress in a direction that impedes future security enhancements.

The technical tasks of WP4 consider these facts when targeting areas of security research with the limited resource available. Hence a focus exists on new security capabilities for tags and readers to solve future application requirements, along with a significant involvement in the developing area of global RFID networks. Where possible in all tasks we use existing technology and standards to combine our efforts with the wider security community, provide confidence in open security standards, and allow interoperability with non-RFID systems.

Task 4.1: Security Analysis and Requirements

An RFID system is composed by multiple components (Tag, Reader, Local Middleware, Network, Application) each of these components requires specific level of security depending on the final applications. Our goal is to provide input to the business work-packages and more in general to end-users and service providers on which security protection mechanisms they should consider.

Will do:

- Capturing security needs and concerns from the other BRIDGE WPs.
- Developing a security analysis.
- Produce a threat model analysis that allows end-user/service provider to measure security threats against their business.

Will not do:

- Define threats for all specific applications.
- Focus solely on privacy issues and end-user concerns related to management of personal identifiable information.

Task 4.2: RFID Tag Security.

Our goal is to focus on research towards secure tags. We will produce prototypes on semi-passive prototype platforms in order to produce future solutions for passive RFID tags. The basic technical work solving the integration of security capabilities on RFID tags will be used to support solutions requiring access control, authentication, confidentiality and data integrity. We are not designing solutions for more capable active RFID tags and sensor devices.

Will do:

- Our mission is to investigate towards application of standardized crypto-primitives on tags and to provide methods and suggestion for secure implementation.
- Provide proof that our concepts and suggestions are feasible by means of semi-passive prototypes.

Will not do:

- Focus on dedicated tag HW development on silicon processes for RFID tags but focus on proof-of-concepts.
- Perform product development for tags, but the results will be directly usable for some niche products in the area of semi-passive solutions (like CAEN or Confidex semi-passive tag).
- Develop solutions for more capable active tags and sensors.

Task 4.3: Anti-cloning of RFID Tags

Research for technologies to provide functionality on tags and readers to fulfil the requirements associated with preventing counterfeiting. These typically are providing methods for a reader to authenticate a secure secret known to the tag.

Will do:

- Development of demo-application using the prototypes and methods developed in T4.2.
- Development of anti-cloning protocol extensions for EPC-gen2
- Cross-platform tests to show platform independence of the developed approaches.

Will not do:

- Investigation of the organizational effort necessary to enable those applications, but we will only investigate and consider extended tag personalization effort in the prototype-application.
- Investigation of legal matters and measures (e.g. compatibility to product pedigree-regulations for pharma-products).

Task 4.4: RFID Trusted Network

Task 4.4 will concentrate on security issues that affect the collection and capture of RFID tag information. In particular, we will concentrate on the development and design of an RFID secure and trusted reader. The goal is to provide a mechanism to control the system integrity and data collection by means of secure local process and operation policies.

Will do:

- Focus on Trusted Computing Platform technology to implement a secure framework for authentication, authorization and accountability.
- Development of a secure reader with CAEN RFID and test in prototype and trials applications.

Will not do:

- Development of Trusted solutions for RFID middleware (ALE) and storage (EPCIS) systems.
- Development of Trusted Computing standards

Task 4.5: Network Confidentiality

Task 4.5 within BRIDGE will concentrate on the security of the inter-organisational or global network. BRIDGE will use existing standard Internet security technologies where these are available. This means we share the efforts of a far wider security community, but is also essential if we consider that RFID systems will not operate in isolation from other services.

Will do:

- Apply existing Internet security standards to collaborative RFID services.
- Investigate appropriate assertions and policies and investigate how these are created across the community.
- Design a Discovery Service in collaboration with WP2 to provide a manageable and scalable solution to the security requirements.

Will not do:

- Create new security protocols and mark-up languages for interaction between RFID service components.
- Develop security solutions for the event collection, processing and internal storage capabilities.

Task 4.6 Data Integrity

Task 4.6 examines some of the security problems faced by applications using the underlying RFID architecture. It will examine some basic techniques that will be applicable to many applications such as the value of automated trust negotiation between parties in the global RFID network. It will also work with WP3 and WP5 to provide techniques for the automatic detection of corrupted, inserted or missing data resulting from security attacks.

Will:

- Investigate the requirement and solutions for developing networks of trust between RFID supply chain participants. Scenarios will be discussed with the BRIDGE business WPs.
- Develop automated trust negotiation processes.
- Detection of anomalous supply chain data through correlation and visualization. Analyse the impact of supply chain visibility on security problems such as theft and counterfeiting.

Will not do:

- Provide complete security solutions for all applications of RFID.

7. RFID Privacy and Data Protection

The BRIDGE WP4 Security work package is concerned with developing research and technical solutions for RFID security. The security work addresses data and process integrity, along with confidentiality of tag and associated business intelligence. BRIDGE does not address consumer privacy specifically, but much of the security work can be applied as Privacy Enhancing Technology within a specific application. Privacy concerns can arise where personal information is stored on RFID tags, or where sightings of such tags can be linked to personal information.

Here we discuss briefly how the BRIDGE security tasks can be applied to the problems of RFID privacy. The discussion is structured using the eight OECD principles of 'Fair Information Practice' [37]. These principles form the basis of much worldwide regulation on data protection and privacy and it can be seen that the EU Directives [38,39,40] follow largely from these principles.

7.1. Collection limitation and security safeguards principle

"There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."

"Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."

The work in BRIDGE on securing the data on the tag and RFID information systems is applicable whether the data concerns personal privacy or sensitive business intelligence. Task 4.2 is developing security techniques that will enable access controls on the tag. Such controls can be used to stop unintended applications obtaining tag information. For example, an ID card of an employee can be secured so that only the legitimate employer can read the tag. The granting of consent should be equivalent to the distribution of the secret required to read the RFID tag. This requires the data subject or trusted party to control the release of such secrets to other parties. For applications with stronger requirements the secrets may only be released in local negotiation with a device of the data subject, or the subject may be required to undertake a consenting action such as enabling the RFID tag.

The work in Task 4.4 on a Trusted RFID Reader provides an alternative to tag access control. Using the Trusted Reader, permitted read policies can be enforced by the reader. The data subject or trusted party may interact with the reader to grant permissions to pass specific RFID data to onward applications. The Trusted Reader may also be used to maintain control over tag secrets where tags with access control are used. In this manner the required secrets may be granted to the Trusted Reader instead of the reader operator or application owner. They may then be easily withdrawn from the reader without requiring the writing of new secrets onto the RFID tag.

Tasks 4.5 and 4.6 deal with the integrity and confidentiality of data exchanged over the network from RFID information systems and applications. It should be clear that techniques to control the spread of sensitive business information also covers the cases where such information may be associated with individuals.

BRIDGE is also concerned with maintaining the integrity of RFID data, both on the tags, and on RFID information networks and systems. Corruption of such data can cause massive disruption to RFID enabled processes. Tag access control can be used to prevent overwriting on the tag data, and similar access controls on information systems can ensure that business of personal data is not corrupted or deleted.

7.2. Data quality principle

"Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."

The support for this principle falls outside the scope of the BRIDGE security workpackage as it deals with data quality and retention. RFID systems should be managed along with other information systems within a business to meet the requirements for data protection and privacy.

7.3. Purpose specification principle & Use limitation principle

"The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."

"Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law."

Before the data is passed to the next onward component in an RFID system, the identity and intention of the onward party should be clear. At the tag level BRIDGE is developing security capabilities on the tag that will allow the authentication of the reader through the presentation of the correct tag secrets. These secrets are only passed to the reader once the purpose has been agreed. The work on the Trusted RFID Reader can also be used to enforce particular processing of the RFID tag data. For example an e-ticketing process can be operated locally on the RFID reader without releasing the raw RFID information to unsecured systems.

BRIDGE is also providing tools to manage the release of RFID data from networked RFID systems. Such release should only occur once the identity of the system is known and

appropriate credentials are supplied. These policies and credentials may specify conditions under which the information is to be released, such as the business role of the data recipient.

7.4. Openness principle & Individual participation principle

"There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."

"An individual should have the right:

a) *to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;*
b) *to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;*
c) *to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and*
d) *to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended."*

These principles fall largely outside the technical research scope of the BRIDGE Security workpackage and are similar for RFID and non-RFID information systems. On the RFID tag itself, the subject should be able to read data from their own tags using the required tag secrets to gain access. Subject should also have the ability using appropriate tag secrets to modify or erase tag data. In the case of un-modifiable data such as the manufacture Tag ID (TID), the tag should be capable of being completely disabled by the subject.

7.5. Accountability principle

"A data controller should be accountable for complying with measures which give effect to the principles stated above."

This principle requires solutions beyond technology. However, security technology can provide tools such as the policing of system behaviour, along with evidence of compliance. Security policies on the RFID information systems can enable transparent and open handling of RFID data and enable auditing of the information flow and purpose.

The Trusted Reader can also be used to enforce RFID data operations in a controlled trusted environment. These operations may involve the processing of RFID data, but can extend to the operation of policing and auditing functions within the RFID data collection network. For example, secure logs may be kept of RFID reading activity.

8. Conclusions

The objective of the report was to review current RFID security activities and investigate future RFID security requirements, with attention being focused on the considered requirements as operational processes move from a closed loop to an open loop EPCglobal network infrastructure, using EPCIS and EPCDS services.

In order to undertake this, the four fundamental layers of an RFID / EPCglobal network infrastructure, (the tag hardware and reader hardware layers, the network layer and the application layer), were investigated with respect to existing and future security requirements / concerns, using literature reviews, detailed interviews and submissions from key players operating within the environment.

The following conclusions regarding current RFID security activities were identified:

- The majority of current applications do not require tags with security functionality but where they do, the majority of tags used are typically active, using proprietary crypto algorithms and undisclosed protocols. These tag designs currently prevent open systems / open review of the security primitives and standardisation, and are therefore inappropriate for use within an open loop EPCglobal network infrastructure.
- Most reader interfaces are defined by the tag specification being read and as such, do not provide authentication to the reader, resulting in the reader accepting whatever identifier or other memory values the tag provides. These values are not processed by the reader but passed to the host for collection and processing, thereby currently limiting the opportunity to perform ‘attacks’ at the reader interface, a situation that will not be duplicated within an open loop EPCglobal network infrastructure.
- With regards to the network, the latest EPCIS candidate specification allows for multiple technology bindings which unlike the lower level interfaces specifies that the binding must provide a means of mutual authentication between the EPCIS and the client, thereby determining authorization to enable access control. The EPCglobal architecture also defines the role of the EPCglobal Subscriber Authentication but for the purposes of BRIDGE, authentication of only EPCglobal subscribers is insufficient as many users of the network will not be EPCglobal subscribers. Authentication of EPCglobal subscribers therefore needs to operate alongside other relevant authentication services.
- Current applications tend to assume high levels of trust in the application provider, and rely on perimeter security (e.g. VPNs) to provide secure environments. Undertaking these applications in the ‘higher’ distributed environment of an open system, will result in exposure to new threats (e.g. Denial of Service attacks), and therefore cannot be allowed to rely solely on network security, and must be based on open standards wherever possible, in order to reduce the cost and complexity of authentication, access control and encryption.

Therefore the purpose and focus of any WP4 activity will be to:

1. ensure that the RFID network and application layers are capable of allowing trusted, secure operations for multiple, unrelated parties, (i.e. within are open system); and,
2. build security functionality into tags and readers to provide applications that can rely on the security provided.

In practical terms, all interviewees agreed that additional security measures would be required if they were to move to an open environment, but none accepted additional security functionality as justification for higher prices, unless a clear business case / requirement existed for the higher level of security provided or the additional functionality provided (e.g. Electronic Article Surveillance). Furthermore, although most interviewees were able to provide detailed information regarding their security concerns, few could translate these into direct technical requirements, as the required level of detail is as yet unknown.

Strong concerns were further expressed with regards to access to item level information and disclosure of potentially confidential information, not only because of the natural concern regarding a third party physically accessing data in an individual's operational system, but more specifically, concerns regarding what secondary activities maybe undertaken with the data obtained (i.e. data analysis, mining etc.).

With regards to the scenarios considered (i.e. product manufacturing, ownership transfer, track and traceability, product verification and product finalisation) and analysed to identify potential security threats associated with moving from an closed to open system, a number of key concerns were identified at each of the relevant architectural layers. These included the cloning tags, the reuse old EPCs, the blocking of readings, the issuing fake reads, the modification of reads, the modification of data, the injection of false data, the interception of data, the blocking of information updates, the issuing of fake orders / confirmation, the denial of service, the changing of EPCs and products, and the ability to access data, a number of which were duplicated within more than one of the said four layers.

With regards to the identified security risks and therefore subsequent security / operational requirements within each of the four layers of the RFID / EPCglobal network infrastructure, the following items were identified as being fundamental to the provision of a secure open loop infrastructure, using EPCIS and EPCDS services.

Areas requiring investigation at the tag layer regarding potential security risks include the physical protection of the tag (including the use of cryptographic access protection and mitigation from a potential physical attack/ side channel attack), protection of the information on the tag (including cryptographic protection), and the compatibility with non-secure RFID reader infrastructures. (Any solution needs to allow the ability for secure tags to be read by insecure readers and vice versa). In addition, the operational security requirements of the tag will need to be considered regarding elements such as tag authentication, reader verification, confidentiality via encryption, tag signature and data access levels.

Areas requiring investigation at the reader layer regarding potential security risks include business process risks (including mitigation of the ability to inject false information), business intelligence risks (including the assurance that confidential information can only be shared

with appropriate third parties), privacy risks (to address the potential for the violation of personal privacy and unwanted surveillance) and security of the IT systems (including the assurance of security at each individual devices to protect integrity and functions).

In order to achieve this, items will need to be provided to ensure software conforms to security and integrity expectations, the ability exists to authenticate the identity and function of a specific reader, that remote integrity checks are possible to ensure readers run specific software builds, and that transponders are supported to ensure a secure environment (including a secure communication protocol for the air interface, a policy management to ensure the reader complies fairly with a specific reading policy and that enhanced security is provided without increasing tag and backend costs).

Areas requiring investigation at the network layer regarding potential security risks will include a determination of the business integrity requirements (to provide a mechanism to check information is valid, accurate and up to date and thereby ensure false information is not introduced into the application), a determination of business intelligence requirements (to enable the disclosure and management of information collected and stored, and prevent activities such as data mining) and a determination of the business privacy risks (to provide access control mechanisms and manage the disclosure of information).

In order to achieve this, items will need to be provided to ensure data integrity, (i.e. that data provided is accurate, complete and up to date), and that parties are held accountable for data they introduce to the system (i.e. so that inaccurate information cannot be introduced into systems via a third party). All relevant data provided will need to be made continuously available, and individuals must be able to access all data relevant to a particular access level. In addition, procedures will need to be in place to ensure track and trace information cannot be used to undertake secondary activities (e.g. data mining), that anonymous queries are controlled, and that data cannot be shared with unauthorised third parties. It is proposed that this requirement will be achieved through the provision of a number of activities, including security audits, non-repudiation of origin requirements, cryptographic key management, user data protection and user identity verification, privacy maintenance and discovery service availability provision.

At the application layer, it is imperative that business processes are not put at risk, hindered or negatively impacted as a result of the proposed security requirements, without a balanced level of business benefit be provided. Security applications must therefore as far as possible be non-intrusive, comply with regulatory requirements, and should not impact the availability or efficiency of internal operational processes.

Items will need to be provided to ensure that data protection and privacy requirements are met and that the trust (whether between individuals, organisations or applications) is maintained. The maintenance of interoperability is paramount (whether inter or intra organisational), as is ensuring that the level of access any individual or organisation has to data / systems within an open loop EPCglobal network infrastructure, meets the required level dictated by the role they perform within the organisation or operation. An auditing capability will also be required to ensure accountability can be determined in the event of any issues / problems.

In order to achieve this therefore, a scalable, non-intrusive authentication and authorisation model will need to be developed, as will the need to investigate the access control mechanisms required to provide the ability to determine the trust level of any external entities requesting access to data, and automatically determine access rights to data objects, dependant on their importance, location and other context information.

From a privacy perspective, many of the outputs of BRIDGE Security work package can be considered as Privacy Enhancing Technologies. Research on confidentiality can be used to control personal information of RFID sighting that may be linked to subjects. Work on integrity can ensure that personal data is not corrupted, while security policies can be used to control the distribution and use of data. However, privacy should not be considered as just a set of technical solutions. Any deployment of RFID should consider the complete system involving regulation, economics, practices and social reaction. Within this framework a solution designer can then consider the technology threats and look for appropriate solutions, which BRIDGE along with other RFID and general security research may provide.

9. References

[1] Soft blocking: flexible blocker tags on the cheap, Ari Juels and John Brainard. WPES 2004.

[2] RFID Malware - Truth vs. Myth, Melanie R. Rieback, Bruno Crispo and Andrew Tanenbaum, IEEE Security and Privacy.

[3] Privacy For RFID Through Trusted Computing, David Molnar, Andrea Soppera, and David Wagner. WPES 2005.

[4] Open Trusted Computing (OpenTC) FP6 consortium - http://www.opentc.net/

[5] BRIDGE Annex I “Description of Work”, 9th August 2006

[6] Security Aspects and Prospective Applications of RFID Systems, Federal Office for Information Security (Germany), 2004

[7] Guidance for Securing Radio Frequency Identification (RFID) Systems (Draft), NIST, U.S. Department of Commerce, 2006

[8] Pim Tuyls, Geert-Jan Schrijen, Boris Skoric, Jan van Geloven, Nynke Verhaegh and Rob Wolters “Read-Proof Hardware from Protective Coatings”, published in Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems 2006 (CHES 2006, October 10 - 13, 2006, Yokohama, Japan), Lecture Notes in Computer Science (LNCS), Springer Verlag, 2006

[9] Kamendje G.-A., Posch R." Intrusion aware CMOS Random Pattern Generator for Cryptographic Applications" In Peter Rössler and Andreas Dörderlein Eds, Proceedings of Austrochip 2001, Vienna)

[10] The EPCglobal Architecture Framework, EPCglobal, July 2005

[11] Ferrailo, D.F., J.F. Barkley, and D.R. Kuhn, *A role based access control model and reference implementation within a corporate intranet.* ACM Transactions on Information Systems Security, February 1999.

[12] Sandhu, R.S., et al., *Role based access control models.* IEEE Computer, 1996. volume 2, February 1996.

[13] Covington, M.J., M.J. Moyer, and M. Ahmad. *Generalized role-based access control for securing future applications*. in *23rd National Information Systems Security Conference*. 2000. Baltimore, MD.

[14] Moyer, M.J. and M. Ahamad. *Generalized Role-Based Access Control*. in *Proceedings of the The 21st International Conference on Distributed Computing Systems*. 2001.

[15] Bardram, J.E., R.E. Kjær, and M.Ø. Pedersen. Context-Aware User Authentication — Supporting Proximity-Based Login in Pervasive Computing. in Proceedings of Ubicomp 2003: Ubiquitous Computing. 2003. Seattle, Washington, USA: Springer Verlag.

[16] Du, W., R. Wang, and P. Ning. *An efficient scheme for authenticating public keys in sensor networks*. in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. 2005. Urbana-Champaign, IL, USA: ACM Press.

[17] Balfanz, D., D. Dean, and M. Spreitzer. *A Security Infrastructure for Distributed Java Applications*. in *Proceedings of 2000 IEEE Symposium on Security and Privacy*. 2000. Oakland, CA.

[18] Minami, K. and D. Kotz, *Secure context-sensitive authorization.* Pervasive and Mobile Computing, 2005. 1, 1: p. 123-156.

[19] Ellison, C.M. *Establishing Identity Without Certification Authorities*. in *Proceedings of the Sixth Annual USENIX Security Symposium*. 1996. San Jose, CA.

[20] Covington, M.J., et al. *A Context-Aware Security Architecture for Emerging Applications*. in *18th Annual Computer Security Applications Conference*. 2002. Las Vegas, Nevada.

[21] Wedde, H.F. and M. Lischka. *Role-based access control in ambient and remote space*. in *Proceedings of the ninth ACM symposium on Access control models and technologies*. 2004. Yorktown Heights, New York, USA: ACM Press.

[22] Flechais, I., M.A. Sasse, and S.M.V. Hailes. *Bringing security home: a process for developing secure and usable systems*. in *Proceedings of the 2003 workshop on New security paradigms*. 2003. Ascona, Switzerland: ACM Press.

[23] van Lamsweerde, A. *Elaborating Security Requirements by Construction of Intentional Anti-Models*. in *Proceedings of the 26th International Conference on Software Engineering*. 2004: IEEE Computer Society.

[24] van Lamsweerde, A., et al., *From System Goals to Intruder Anti-Goals: Attack Generation and Resolution for Security Requirements Engineering*. 2003.

[25] Kim, S.-K. and D. Carrington. *Integrating Use-Case Analysis and Task Analysis for Interactive Systems*. in *Proceedings of the Ninth Asia-Pacific Software Engineering Conference*. 2002: IEEE Computer Society.

[26] Thiesse, F., *Managing Risk Perceptions of RFID*, Auto-ID Labs White Paper

[27] ISO/IEC 10746: 1996. “Information technology - Open Distributed Processing - Reference Model: Foundations”.

[28] ISO/IEC 15408: 2005. “Information technology – Security Techniques – Evaluation criteria for IT security”.

[29] David F. Ferraiolo and D. Richard Kuhn, "Role-Based Access Controls," Proceedings of the 15th NIST-NSA National Computer Security Conference, Baltimore

[30] D.L. Chaum, ``Untraceable electronic mail, return addresses, and digital pseudonyms,'' *Communications of the ACM* 24(2), 84-88 (1981)

[31] Ye, S., F. Makedon, and J. Ford. *Collaborative Automated Trust Negotiation in Peer-to-Peer Systems*. in *Proceedings of the Fourth International Conference on Peer-to-Peer Computing (P2P'04)*. 2004: IEEE Computer Society.

[32] Hess, A., et al., *Content-triggered trust negotiation.* ACM Transactions on Information and System Security, 2004. 7, 3: p. 428-456.

[33] English, C., P. Nixon, and S. Terzis. *Dynamic trust models for ubiquitous computing environemnt*. in *Proceedings of Ubicom 2002*

[34] Irwin, K. and T. Yu. *Preventing attribute information leakage in automated trust negotiation*. in *Proceedings of the 12th ACM conference on Computer and communications security*. 2005. Alexandria, VA, USA: ACM Press.

[35] Winsborough, W.H. and N. Li, *Safety in automated trust negotiation.* ACM Transactions on Information and System Security, 2006. 9, 3: p. 352-390.

[36] Winsborough, W.H. and N. Li. *Towards Practical Automated Trust Negotiation*. in *Proceedings of the Third International Workshop on Policies for Distributed Systems and Networks*. 2002. Monterey, CA.

[37] OECD — Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, (September 1980).

[38] EU Directive 1995/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (October 1995).

[39] EU Directive 1997/66/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, December 1997.

[40] EU Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, (July 2002).

Appendix A – Security Requirement Summary

Requirement Taxonomy

Security Concern	Tag-Layer	Reader Layer	Network-Layer	Application-Layer
Authentication	REQ_TAG_1	REQ_REA_1	REQ_NET_1	REQ_APP_1
Confidentiality	REQ_TAG_2	REQ_REA_2	REQ_NET_2a REQ_NET_2b	REQ_APP_2
Availability	REQ_TAG_3	*Not applicable*	REQ_NET_3	REQ_APP_3
Privacy	REQ_TAG_4	REQ_REA_4a REQ_REA_4b	REQ_NET_4	REQ_APP_4
Non-repudiation	REQ_TAG_5	*Not applicable*	REQ_NET_5	REQ_APP_5
Access Control	*Not applicable*	REQ_REA_6	REQ_NET_6	REQ_APP_6
Integrity	REQ_TAG_7	REQ_REA_7	REQ_NET_7a REQ_NET_7b	REQ_APP_7a REQ_APP_7b
Interoperability	REQ_TAG_8	REQ_REA_8a REQ_REA_8b	REQ_NET_8	REQ_APP_8

Tag-Layer

ID	**REQ_TAG_1**
Summary	Authentication
Rationale	Business Integrity
Requirement	A tag that supports tag authentication must provide a proof of its identity by cryptographic measures. Reader authentication must be verified for applications that need access restrictions to the tag's memory or functionality
References	D4.1.1 – Use Case Scenario – Product Verification
Originator	TUG
Taxonomy	Tag-Layer

ID	**REQ_TAG_2**
Summary	Confidentiality
Rationale	Business Integrity
Requirement	Communication between tag and reader must be encrypted for applications that need to prevent eavesdropping of the contact-less channel.
References	D4.1.1 – Use Case Scenario – Product Verification
Originator	TUG
Taxonomy	Tag-Layer

ID	**REQ_TAG_3**
Summary	Availability
Rationale	Business Integrity
Requirement	Tags should not be disabled when product is being used by business process.
References	D4.1.1 – Use Case Scenario – Product Verification
Originator	TUG
Taxonomy	Tag-Layer

ID	**REQ_TAG_4**
Summary	Privacy
Rationale	Business Intelligence
Requirement	After a product is sold to the final user the tag attached must be capable of being disabled.
References	D4.1.1 – Interview – Consumer privacy
Originator	TUG
Taxonomy	Tag-Layer

ID	**REQ_TAG_5**
Summary	Non-repudiation
Rationale	Business Intelligence
Requirement	A reader that includes signature functionality must request that a tag signs information sent to it. After signature a reader can proof that a specific tag has communicated with the reader.
References	D4.1.1 – Use Case Scenario – Product Verification
Originator	TUG
Taxonomy	Tag-Layer

ID	**REQ_TAG_7**
Summary	Integrity
Rationale	Business Integrity
Requirement	Tag must be secured against malicious writing of EPC.
References	D4.1.1 – Use Case Scenario – Product Manufacturing
Originator	TUG
Taxonomy	Tag-Layer

ID	**REQ_TAG_8**
Summary	Interoperability
Rationale	Operational and Deployment
Requirement	It must comply with EPC, but maybe with temporary IDs, or restrict access to some protected memory only to authenticated readers. This allows application of secure tags in standard supply chains, but makes secure operation (e.g. after POS) possible.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	TUG
Taxonomy	Tag-Layer

Reader-Layer

ID	REQ_REA_1
Summary	Authentication
Rationale	Business Intelligence
Requirement	It is needed to have mechanisms in place to authenticate the identity and the function of a specific reader.
References	D4.1.1 – Use Case Scenario – Product Transfer
Originator	BT
Taxonomy	Reader-Layer

ID	REQ_REA_2
Summary	Confidentiality
Rationale	Business Intelligence
Requirement	The reader must be able to identify in which way the information is encoded and implement different protocols simultaneously.
References	D4.1.1 – Use Case Scenario – Product Verification
Originator	BT
Taxonomy	Reader-Layer

ID	REQ_REA_4a
Summary	Privacy
Rationale	Business Intelligence
Requirement	The reader must be able to identify which secret should be applied to encoded information. The right password or shared secret should be provided to the right reader with secure communication.
References	D4.1.1 – Use Case Scenario – Product Verification
Originator	BT
Taxonomy	Reader-Layer

ID	REQ_REA_4b
Summary	Privacy
Rationale	Business Intelligence
Requirement	The secret information required to decode the tag must be maintained in a secure memory part of the reader. A secret can not be disclosed to the wrong application, user or reader owner
References	D4.1.1 – Use Case Scenario – Product Verification
Originator	BT
Taxonomy	Reader-Layer

ID	REQ_REA_6
Summary	Access Control
Rationale	Business Intelligence
Requirement	The reader must implement access control on any interfaces that allow the modification of reader operation or access to internal information.

References	D4.1.1 – Interview – Security of internal IT-Systems
Originator	BT
Taxonomy	Reader-Layer

ID	**REQ_REA_7**
Summary	Integrity
Rationale	Business Integrity
Requirement	Injection of data from readers needs to be controlled in order to avoid the data corruption with false information.
References	D4.1.1 – Interview – Injection of false information
Originator	BT
Taxonomy	Reader-Layer

ID	**REQ_REA_8a**
Summary	Interoperability
Rationale	Operational and Deployment
Requirement	It's mandatory to provide a mechanism to guarantee that the RFID reader complies with a specific reading policy in support of fair information practice principles.
References	D4.1.1 – Interview – Disclosure of confidential information
Originator	BT
Taxonomy	Reader-Layer

ID	**REQ_REA_8b**
Summary	Interoperability
Rationale	Operational and Deployment
Requirement	Secure reader should be able to operate with secure and insecure RFID tags.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	BT
Taxonomy	Reader-Layer

Network-Layer

ID	**REQ_NET_1**
Summary	Authentication
Rationale	Business Intelligence
Requirement	Mutual authentication between the parties which takes part in EPC data communication. Both party sender and receiver must trust each other by using a large size scalable authentication infrastructure.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP and BT
Taxonomy	Network-Layer

ID	**REQ_NET_2a**
Summary	Confidentiality
Rationale	Business Intelligence
Requirement	The data is only released to those who disclose their valid identity. The information exchanged among elements must be available only for those who are mutually authenticated by using a scalable confidential architecture.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP and BT
Taxonomy	Network-Layer

ID	**REQ_NET_2b**
Summary	Confidentiality
Rationale	Business Intelligence
Requirement	The external transaction through the interfaces among DS and other parties, i.e., queries and updates must be confidential with accordance to the security polices established which should set the fields of the DS record to be protected.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	AT4 wireless
Taxonomy	Application-Layer

ID	**REQ_NET_3**
Summary	Availability
Rationale	Operational and Deployment
Requirement	EPICS systems must be resilient to Denial of Service attack and provide back-ups facilities in order to avoid unavailability at any time.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP and BT
Taxonomy	Network-Layer

ID	**REQ_NET_4**
Summary	Privacy
Rationale	Business Intelligence

Requirement	A party may need not to disclose its real identity. The EPC network elements must implement access control and authentication mechanism by which anonymous data transactions can be feasible,
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP and BT
Taxonomy	Network-Layer

ID	**REQ_NET_5**
Summary	Non-repudiation
Rationale	Business Intelligence
Requirement	Data contributions to the system must be signed in order that individual parties can me held accountable for the quality of the data they provide.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP and BT
Taxonomy	Network-Layer

ID	**REQ_NET_6**
Summary	Access Control
Rationale	Business Intelligence
Requirement	Information shares must own the capability to specify the conditions under which they want to share the data. These rules must be managed by sound access controls mechanism.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP & BT
Taxonomy	Network-Layer

ID	**REQ_NET_7a**
Summary	Integrity
Rationale	Business Integrity
Requirement	Only authorized parties must be allowed to register their EPC ISs with a DS in such a way that parties can not be injected selfishly and inaccurate information into the system.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP and BT
Taxonomy	Network-Layer

ID	**REQ_NET_7b**
Summary	Integrity
Rationale	Business Intelligence
Requirement	Depending on a client's access rights, 'all' the data at different levels of visibility must be able to be accessed. In order to prevent from data inconsistency the information must be up-to-data,.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP and BT
Taxonomy	Network-Layer

ID	**REQ_NET_8**
Summary	Interoperability
Rationale	Operational and Deployment
Requirement	Network components should be built upon existing standards and frameworks for identity and access control.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP and BT
Taxonomy	Network-Layer

Application-Layer

ID	REQ_APP_1
Summary	Authentication
Rationale	Business Intelligence
Requirement	Users must own a single credential whereby must authenticate to the application to which want to get granted access.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP
Taxonomy	Application-Layer

ID	REQ_APP_2
Summary	Confidentiality
Rationale	Business Intelligence.
Requirement	Interfaces should assure confidentiality in the exchange data between the applications and the network services.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	AT4 wireless
Taxonomy	Application-Layer

ID	REQ_APP_3
Summary	Availability
Rationale	Business Intelligence.
Requirement	DS must be able to provide mechanism whereby prevent users from monopolising the resources.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	AT4 wireless
Taxonomy	Application-Layer

ID	REQ_APP_4
Summary	Privacy
Rationale	Business Intelligence
Requirement	The parties interacting with DS can not be aware from the usage of DS and whether or not another party is querying or updating the DS must be also hidden.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	AT4 wireless
Taxonomy	Application-Layer

ID	REQ_APP_5
Summary	Non repudiation
Rationale	Business Intelligence
Requirement	The parties which update DS records must be accountable for this fact. Likewise, the responsibility which the parties own in order not to refuse having receive queries at any time.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	AT4 wireless
Taxonomy	Application-Layer

ID	**REQ_APP_6**
Summary	Access Control
Rationale	Business Intelligence
Requirement	Employee and application user must own an access rights depending on the roles assigned by the valid authority in charge of the EPC application.
References	D4.1.1 – Interview – Missing Control of Information
Originator	SAP
Taxonomy	Application-Layer

ID	**REQ_APP_7a**
Summary	Integrity
Rationale	Business Integrity
Requirement	Privacy concerns of companies and customer must be achieved by assuring the integrity of the relevant data collected.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP
Taxonomy	Application-Layer

ID	**REQ_APP_7b**
Summary	Integrity
Rationale	Business Integrity
Requirement	In order to facilitate the feasibility of REQ_APP_3, the collected data must fulfil the following features: - Data collected should be adequate, relevant, and not excessive. - Data should not be kept longer that necessary. - Companies and customers have the right to know data about them or their products is stored. - Data collected should be processed for a specific purpose (e.g. data mining to infer new, unauthorized data shouldn't be permitted or feasible.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP
Taxonomy	Application-Layer

ID	**REQ_APP_8**
Summary	Interoperability
Rationale	Operational and Deployment
Requirement	Even though any new security mechanisms and trust models affect the in place mechanisms and the current applications and in order to avoid high cost application migration, the interoperability should not only considered at intra-organizational level.
References	D4.1.1 – Use Case Scenario – Track and Trace
Originator	SAP
Taxonomy	Application-Layer