Building **R**adio frequency **ID**entification for the **G**lobal
Environment

The Economic Relevance of Secure RFID Solutions – a Qualitative Perspective (D.4.1.3)

Authors: Manfred Aigner (TU Graz), Trevor Burbridge (BT Research), Jeff Farr (BT Research), Alexander Ilic (ETH Zurich), Robert Maidment (GS1-UK), Florian Michahelles (ETH Zurich)

December 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 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.

This document:

The WP4 "Security" work package of BRIDGE is examining ways to ensure that RFID tags, readers, network infrastructure, and RFID services are developed in harmony with security features to enable effective and safe deployment of applications in various business sectors.

However, some organizations tend to see security as nothing more than an extra feature or a "nice to have" for RFID deployments. To these stakeholders, the real economic value of security is often obscure. We provide a sound discussion, based on case studies, to outline that secure RFID solutions are more than just an add-on and are in fact an essential pre-requisite to many, especially open-loop deployments. As the most radical RFID applications are only successfully if supply chain partners are willing to participate and share information that was previously considered proprietary, security features are needed as a necessary insurance mechanism. But security technologies offer even more: we provide case studies that show that secure RFID solutions allow for the deployment of completely new business applications. Without proper security features in place, these applications would be impossible to launch.

The case studies show that there are potentially huge business benefits that cannot be leveraged today because of a lack of adequate security. Secure RFID solutions do not just fix problems induced by RFID technology itself, but also enable new applications and the deployment of RFID in open-loop environments. They lower entry adoption barriers, mitigate risks and enable new innovative processes. Work Package 4 positions itself to pursue developments that push these kind of secure RFID solutions forward.

Disclaimer:

This document contains preliminary information and is not subject to any license agreement or any other agreement as between with respect to the above referenced consortium members. This document contains only intended strategies, developments, and/or functionalities and is not intended to be binding on any of the above referenced consortium members (either jointly or severally) with respect to any particular course of business, product strategy, and/or development of the above referenced consortium members. To the maximum extent allowed under applicable law, the above referenced consortium members assume no responsibility for errors or omissions in this document. The above referenced consortium members do not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, or non-infringement. No licence to any underlying IPR is granted or to be implied from any use or reliance on the information contained within or accessed through this document. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intentional or gross negligence. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you. The statutory liability for personal injury and defective products is not affected. The above referenced consortium members have no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages.

Abstract

The WP4 “Security” work package of BRIDGE is examining ways to ensure that RFID tags, readers, network infrastructure, and RFID services are developed in harmony with security features to enable effective and safe deployment of applications in various business sectors.

However, some organizations tend to see security as nothing more than an extra feature or a “nice to have” for RFID deployments. To these stakeholders, the real economic value of security is often obscure. We provide a sound discussion, based on case studies, to outline that secure RFID solutions are more than just an add-on and are in fact an essential pre-requisite to many, especially open-loop deployments. As the most radical RFID applications are only successfully if supply chain partners are willing to participate and share information that was previously considered proprietary, security features are needed as a necessary insurance mechanism. But security technologies offer even more: we provide case studies that show that secure RFID solutions allow for the deployment of completely new business applications. Without proper security features in place, these applications would be impossible to launch.

The case studies show that there are potentially huge business benefits that cannot be leveraged today because of a lack of adequate security. Secure RFID solutions do not just fix problems induced by RFID technology itself, but also enable new applications and the deployment of RFID in open-loop environments. They lower entry adoption barriers, mitigate risks and enable new innovative processes. Work Package 4 positions itself to pursue developments that push these kind of secure RFID solutions forward.

Relation to other deliverables

This deliverable is the third and final deliverable of task 4.1 of Work Package 4 (WP4) "Security". The already completed deliverables D-4.1.1 and D-4.1.2 have discussed security threats and requirements for retailers, suppliers, consumers and other stakeholders. We have analyzed the current state of the art technology and discussed the security challenges that we need to overcome in order to enable the deployment of value-adding inter-organizational RFID applications. In particular, we have studied the risks and threats for RFID enabled supply chains, including the analysis of risks and threats for SMEs. The role of task 4.1 is to provide an information basis and joint perspective for the other tasks in WP-4 that focus on the research and development of the technical solutions. In this manner, the associated deliverables D-4.2.1, D-4.3.1, D-4.4.1, D-4.5.1 and D-4.6.1 are concerned with researching and developing tag, reader and network infrastructure security (cf. Figure 1). Therefore, this report will focus on discussing the benefit side of a complete secure RFID solution. We provide a joint perspective of work package WP4 to outline the economic relevance of security and will refer to the other deliverables for further technical details.

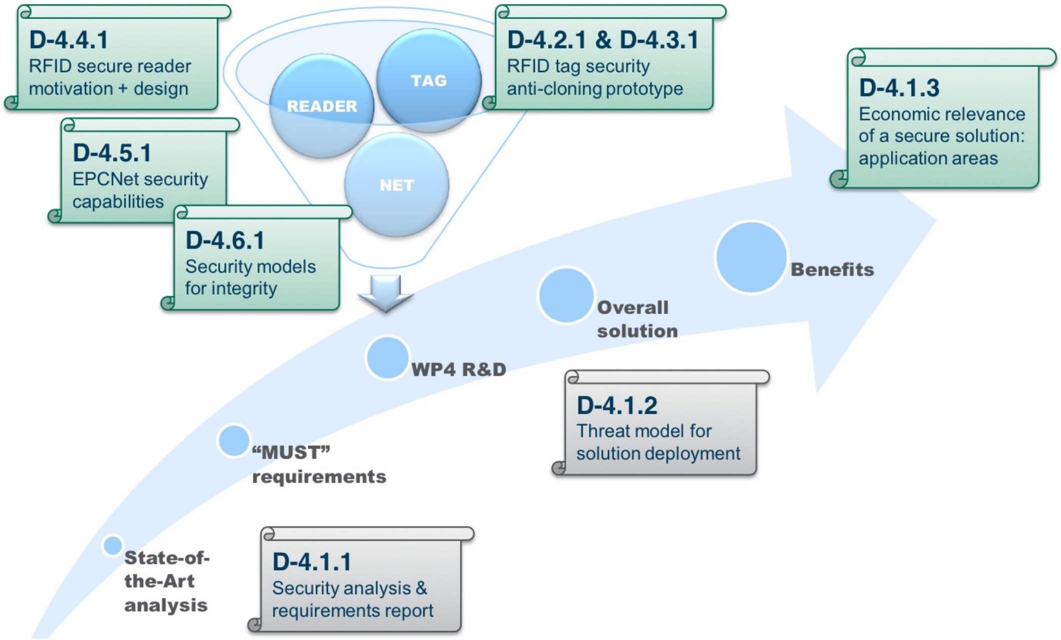
D-4.4.1
RFID secure reader motivation + design
D-4.5.1
EPCNet security capabilities
D-4.6.1
Security models for integrity
READER
TAG
NET
D-4.2.1 & D-4.3.1
RFID tag security anti-cloning prototype
D-4.1.3
Economic relevance of a secure solution: application areas
Benefits
Overall solution
WP4 R&D
D-4.1.2
Threat model for solution deployment
"MUST" requirements
State-of-the-Art analysis
D-4.1.1
Security analysis & requirements report

Figure 1. WP4 deliverables till M18 and their relationship to each other

1. INTRODUCTION 7

1.1. MOTIVATION 7
1.2. BACKGROUND 8
1.3. GOALS AND METHOD 8

2. CASE STUDIES 10

2.1. E-PEDIGREE 10
2.2. TRACK- AND TRACEABILITY 10
2.3. RETURNABLE TRANSIT UNITS 11
2.4. DIRECT TRACEABILITY ACROSS SUPPLY-CHAIN PARTNERS 11
2.5. ENABLING LOSS ACCOUNTING OF POOLED RTIS 12
2.6. ENABLING ANTI-COUNTERFEITING THROUGH CLONE-PREVENTION TAGS 13

3. TECHNOLOGY CUT 15

4. CONCLUSIONS 16

5. REFERENCES 17

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 System
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 Motivation

RFID is a disruptive technology that has a huge potential to change management activities, due to its ability to automate processes and provide accurate, trusted data [1]. Its unique features include the ability to give each physical object a globally unique digital identity which can be read from a distance without requiring line-of-sight and in case of passive RFID, to operate even without a battery [2]. These features provide new ways of measuring and integrating the real world into information systems and because of this, RFID has great potential to change the way we do business. From a security perspective, the three effects depicted on Figure 2 are relevant to consider.

First, when RFID is implemented to improve an existing business process [1], RFID can enable the automation of activities and thereby reduce the potential business and security risks caused due to human error. Second, RFID itself induces new risks to a process [3]. Security is therefore needed to keep automated aspects and invisible properties under control, otherwise the process could be susceptible to mass abuse. Third, RFID itself can enable completely new business applications [4] due to its properties as a data gathering and process measurement technology. Activities and actions that could not accurately be measured before can now be measured. Again, security plays a major role here, as it provides the accountability needed to enable trust in the data and activities provided by these applications.

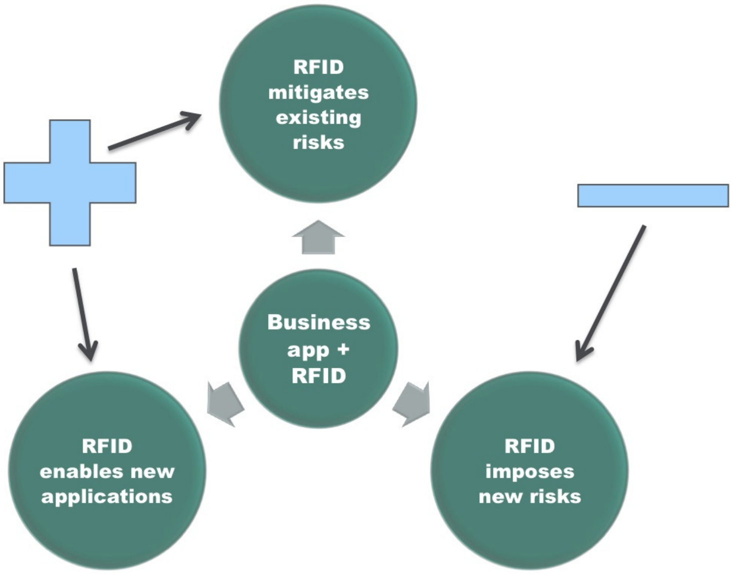

Figure 2. WP4 tries to improve the balance between risks and benefits of RFID-based business applications by developing secure RFID solutions

From a work package 4 (WP4) perspective, the goal is to provide security technology that supports the potential of RFID in mitigating existing business and security risks in processes while at the same time enabling the inherent security problems of the RFID technology to be managed. In addition, we believe that security is not only a must for business cases where RFID improves an existing barcode scenario, but also a completely new opportunity. Applications that are not possible to deploy today as their critical points depend mainly on security, will benefit from the technology developed in WP4 [5]. Secure RFID solutions are not just a must, but also an enabler of powerful applications that can increase the competitiveness of organizations tremendously.

1.2 Background

The need for continuous improvement and competitive advantage requires organisations to make informed decisions based on accurate and timely operational data gathered not only in one's own facilities, but also provided via unrelated third parties. Based on low-cost 'track and trace' data gathering technologies such as RFID, industry is now making a big step towards developing global standards for the sharing of operational data traces. The not-for-profit organization EPCglobal has already developed a number of important standards[1] (EPC Gen-2/ISO18000-6C, Low-Level Reader Protocol, Application-Level Events, EPC Information Services, Object Naming Services) and aims to further standardise and complete the so-called EPC Network Architectural Framework[2] to enable the seamless gathering, filtering, and sharing of 'track and trace' data on a global scale. EPCglobal is a not-for-profit organization that is driven by its member companies, which work together via so-called Joint-Requirement-Groups (cross-industry) and Business-Action-Groups (industry specific), as well as Hardware and Software Action Groups, to develop industry driven, globally acceptable standards. The members (now over 1400 companies) comprise a balanced mixture of solution providers and end-users such as Wal-Mart, Nestle, Carrefour, Metro, GE, Pfizer, and Procter & Gamble. With the recently standardised EPC Information Services (EPCIS)[3], EPC-based information sharing networks are said to play a major role in improving future supply chain efficiency and have the potential to revolutionize the management of supply chain networks.

EPC-based information sharing networks facilitate the processing and exchange of item-level and consignment level 'track and trace' data through the use of low-cost radio frequency identification (RFID) tags. In contrast to standalone RFID middleware systems, the application areas are not limited to closed-loop scenarios, but also to inter-organizational open-loop processes [5]. In contrast to closed-loop processes, open-loop RFID processes support 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, not for a long period of time and usually only for end-of-life processes. Hence, open standards are required to enable seamless data exchange among participants. As businesses begin to rely on EPC-based events to manage and to share critical supply chain processes, security solutions investigated by the BRIDGE project need to be in place to guarantee control of confidential data and system accountability. Sharing information can increase productivity, but also introduces questions about the use and misuse of information by third parties once information has been disclosed.

1.3 Goals and Method

The goal of this deliverable is to highlight the economic relevance of secure RFID solutions. Particularly we want to show that there is more to security than just fulfilling a must. As the high level goal is to leverage the benefits of RFID, we will not just focus on the improvement of existing business cases but also show that secure RFID solutions can enable completely new and innovative applications. These applications require that "supply chain partners are willing to participate and share information that was previously considered proprietary" [4]. Therefore, we believe that without complete and secure RFID solutions, the full potential of

[1] http://www.epcglobalinc.org/standards

[2] http://www.epcglobalinc.org/standards/architecture

[3] http://www.epcglobalinc.org/standards/epcis

RFID can never be unlocked. To support our hypotheses, we will employ exemplary case studies that support our line of argument.

To achieve the aforementioned goals, this deliverable is structured as follows. Section 2 analyzes case studies in the categories of 1) advancing existing barcode applications and 2) enabling new applications with regard to security. Section 3 presents the technology spectrum of secure RFID solutions and outlines how we believe that, in principle, the problems elaborated in the case studies can be overcome. This deliverable closes with Section 4 to draw conclusions and present final remarks.

2 Case Studies

In the following we will study the benefits of RFID and the involved necessity for applying appropriate security mechanisms by means of selected case studies.

The first three cases describe business scenarios that have already been implemented using barcode technology but which can be improved by using RFID technology. In all three cases the advantages of RFID over barcodes are that:

- RFID has the ability to automate the monitoring of product movements in supply-chains
- RFID readings are more accurate than (mostly manually operated) barcode systems
- RFID tags can be integrated within the structure of packaging material or even within products.

In contrast, the remaining cases in Section 2.4, Section 2.5, and Section 2.6 show that RFID security can also enable completely new applications, which mostly rely on RFID's characteristic of implementing new security mechanisms.

2.1 e-Pedigree

The principle of e-pedigree is for every player involved in the movement of a consignment (e.g. medicines) through a supply chain to provide a 'digitally signed certificate' confirming and authenticating all activities undertaken whilst in possession of the consignment, the 'certificates' compounding as the consignment moves along the process between players, providing a fully certified audit trail of the consignments activities, thereby providing the end user with proof of the consignments authenticity on arrival at its final destination.

In November 2006 the European Federation of Pharmaceutical Industries Associations (EFPIA) promoted the introduction of 2D barcodes that uniquely identify single packages. RFID has the ability to store dynamic data, which can add current and object-specific information (e.g. serial number, date, time, location) to the product. Furthermore, due to the higher degree of automated read and write processes RFID enables, the progression of operational process throughout the supply-chain can be monitored more frequently. Consequently, it can provide a more fine-grained audit trail which, as such, results in a higher level of protection against attempts of illicit actors to fake audit trails.

As e-pedigree is generally used to manage valuable, highly sensitive products, it is imperative that the integrity of the certificates and data provided can be trusted and protected at every stage. RFID can provide a higher level of security by providing mechanisms against the cloning of tags, whereas barcodes can be photocopied easily. The higher level of protection and automation through RFID was one of the key arguments for the American food and drug administration (FDA) to recommend RFID technology for the implementation of e-pedigree solutions [8].

2.2 Track- and Traceability

There are numerous supply chains which due to the value and sensitivity of the consignment, require accurate process management and audit trail provision, whether that be due to their security requirements (e.g. mobile telephones, artwork etc.), their need for precise management (e.g. clinical trials, public health toxicity testing etc.) or compliance with legislative requirements (e.g. taxation on cigarettes, alcohol etc.).

The ability of RFID to provide more reading points at lower costs via automated reading stations, checking activities against pre-set parameters, significantly adds to the quality of service of such a system.

In addition, the removal of reliance on human operators to control the process and the subsequent management of the process by the automated system, means that it is imperative that all data on which the process is acting and information provided, can be trusted to be secure and accurate by all players. Thus, security mechanisms for RFID have to protect against threats, such as injection of false information, denial of service attacks and sniffing in order to guarantee the credibility of such a system. Without those security features, using such a system has no value.

2.3 Returnable Transit Units

The movement of many of the above mentioned products through a logistical supply chain is frequently dependent on the use of Returnable Transit Units (RTU) as the medium for their transportation. From a cost perspective, tagging a RTU is particularly appealing as the costs of RFID tags (and any additional sensors) amortize over its long lifetime. The movement of the RTU is frequently the method via which the movement of the consignment's products is managed, via 'association' (as opposed to monitoring the movement of the actual products themselves). As the RTU is therefore the fundamental element on which the movement of product (and payment if loaned) and therefore the business is dependent, it is imperative that the progression, location and organisation responsible at any particular point in time for the RTU is known, to ensure that assets are used efficiently and that any responsibility for damage, loss, delay etc. which will effect the business can be accurately determined.

The user and process players will only accept such a system if all data on which the system is making process related decisions, as well as any business related information provided by the system, can be trusted to be a true and accurate reflection of reality. It is therefore imperative to ensure that all data collation, information management and provision is accurate and secure, and to ensure that individual players and / or third parties cannot corrupt, remove, or add data etc., or use data to undertake 'data mining' based analysis of activities to the unfair detriment of other players, resulting in economic or business loss to end users / other players.

2.4 Direct Traceability across supply-chain partners

In section 2.2 we examined how traceability restricted to the control of single organizations can be achieved. However, legislative regulations demand many supply-chains (food industry, automotive parts, aerospace industry, etc.) to keep track of items throughout their entire lifecycle. Today, supply chain information, or at least references to the data, are passed from one partner to the other, typically as the physical goods also flow along the supply chain. Queries about goods are similarly passed from one partner to the next until, hopefully, they reach a point where an answer exists. The obvious drawback of this cascaded approach is that all of the partners have to participate, regardless of any individual benefit they receive. A distributor must relay data or queries between a manufacturer and a retailer even if they have no direct interest in such a process. If just one participant is unwilling or unable to participate, then the flow information is severely disrupted. Even with complex security controls, some level of trust exists in the intermediate partners of the supply chain (minimally to route the data or query correctly).

An alternative approach is to establish a registry service, either as a shared network or third-party operated service that enables direct traceability. RFID technology is used to collect supply chain data which is shared among partners by using the standards of the EPCglobal network architectural framework. Queries for supply chain information related to certain physical items are forwarded to a Discovery Service to resolve which supply chain participants hold information relevant to that query. The simplest Discovery Service may only hold a reference to the partner's information repository such as an EPCIS, and may only allow queries keyed on the EPC. Richer traceability services may hold far more data, allow complex queries over other attributes (such as location), and perform reasoning over historical data (such as predicting when and where the product will be seen next).

None of these services will emerge unless security is adequate. A producer of supply chain information needs to be able to protect the confidentiality of the data. Otherwise they will leak sensitive business intelligence and loose any economic value associated with the data. The value of sharing the data must be lower than the risk to the organisation by doing so. Controlling the flow of information to just the next partner or Discovery Service will not be adequate, since we need to retain control of the ultimate destination. If such controls are not secure, are too costly to implement, or are too complex to manage, then producers of information will release such information only to a select group of parties for whom they have higher confidence and business benefit. Even if one could get producers of supply chain information to share their data in a controlled fashion, that is not the end of the story. Information is useless unless we can operate some process or make some decision based upon it. Receiving supply chain data from others therefore exposes an organisation to potentially huge risks of supply chain process disruption. If the information in the system is worthless or even worse has a higher risk than benefit, then direct traceability systems will fail. Consumers of traceability data need confidence that the data originates from the expected source and has not been tampered with. Techniques such as authentication and digital signatures can provide answers. Furthermore, they may also require contracts that guarantee the quality of the data and offset the risks to their organisation. To enact such contacts requires legally enforceable accountability and non-repudiation. Providing the security of traceability services is well designed and the costs of implementation and management are low, then such services may be introduced initially for low economic advantages. As more data becomes reachable and confidence in the data grows, then traceability services will provide a stepping-stone to new radical services and applications.

2.5 Enabling Loss Accounting of pooled RTUs

RTUs (such as pallets, crates, and plastic boxes) are widely used within supply chains to transport products across multiple supply chain partners. The RTUs themselves are usually owned by one of the supply chain parties, or may be hired from a third party 'RTU Pool Provider' (e.g. Euro Pool Systems). But often, they may be handled, moved, stacked, loaded, unloaded, transported, mis-placed, stolen, and even damaged by many other supply chain parties. The figure below shows an exemplar use-case for a pallet transporting items from a Manufacturer to a Retailer. Owners of such RTUs would like to monitor (and ultimately control) the use of these assets more effectively. For example, they would like more accurate information on the average cycle rotation rates (the period of time it takes an RTU to complete a single usage cycle, see figure), and they would like to monitor others' use of their RTUs more accurately. They would especially like to be able to hold other parties more accountable for the use they make, and damage they might cause, to the RTUs. Whilst normal 'wear and tear' damage might be acceptable, the owners would often like to trace, and possibly charge those who accidentally or deliberately damage, contaminate or soil their RTUs. Cleaning and repairing RTUs is an expensive process, and some businesses mandate the use of certifiably-clean RTUs for transporting their products.

By RFID-enabling each RTU, and tracking and monitoring its usage throughout the supply chain with an EPC Network (Readers, ALE, EPCIS and possibly Discovery Services), it would seem that these business goals could be realised. Indeed, there are a number of RTU Pool Providers currently investigating exactly such a vision (e.g. SmartFlow Pooling & LPR (within the context of WP9); Container Centralen).

However, such a system clearly relies upon accurate, truthfully declared-data. For example, it relies upon the fact that parties accurately report the times at which they receive, and dispatch the RTUs, and that they accurately report any damage as soon as it occurs. Unfortunately, the other parties have an inherent, selfish motivation not to do so. They will almost always benefit (or at least, avoid additional costs) if they under-estimate the period of time for which they have possession of an RTU, or if they under-report damage that occurs during their custodianship. The success of the whole system relies upon the integrity of the data provided. An initial suggestion to help 'accurately record' damage to an RTU might be to install a sensor-enabled RFID tag on it, so that (say) physical shock from mis-use can be directly recorded. However, without adequate security mechanisms it might be extremely easy for a selfish party to manipulate or erase the data, and so corrupt the final system. There is thus a strong need to accurately capture and then maintain the integrity of the information used in this system. Mechanisms that help maintain the integrity of the EPC Network-based information are thus a critical part of this system.

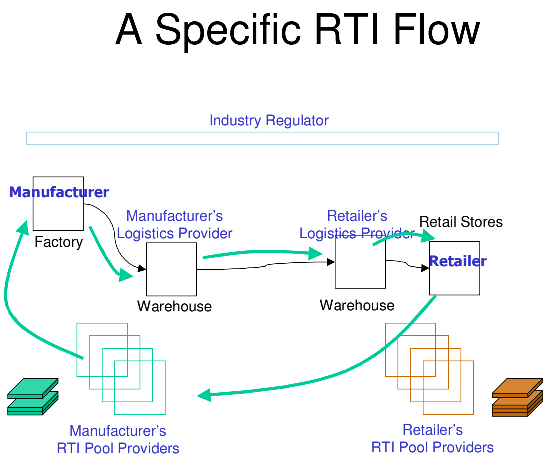

Figure 3. A Specific RTU Flow

There are two other security elements of critical importance to this system. Firstly, it is clearly essential that parties can be held accountable for the information they provide. This is the property of non-repudiation, and is easily provided by digital signing. Secondly, it is quite feasible that the information captured (about RTUs) could be used to infer commercially-sensitive business knowledge about the goods, or supply chain parties themselves. For example, it could easily, and accurately, be used infer the time taken by goods to travel between two locations, or to assess when and where damaged goods might be found. Many companies are extremely concerned that the information they capture might be mis-used in such ways, and so there is a strong need to ensure that an appropriate degree of information confidentiality can be maintained.

It should be clear that, in this case, ensuring the security of the EPC Network is not a helpful, optional, addition but an essential requirement in order to make this new RTU management model possible. This RTU scenario is explored more deeply, and a set of solutions are proposed, in the accompanying WP4 Month 18 Deliverable Report D-4.5.1.

2.6 Enabling Anti-Counterfeiting through Clone-Prevention Tags

Off-line checks for authenticity can be an added value for the customer. Offline means, that no network access should be necessary for the authentication. In the case that tags allow cryptographic operation, such checks are feasible. In the case that symmetric cryptography is available on tag, the verifier needs access to the key, or to a service that provides “valid” challenge-response pair.

It is important to note, that such checks need to be secured against attacks, since a successful check for authentication may justify a higher price for an object (you might be willing to pay more money for e.g. your medicine or your replacement ABS sensor, if you can be sure that the product is what it claims to be), therefore a negative check for an original product is potentially damaging. It is not enough for many applications that clone tags in the supply chain are detected, but it is also important that clones are prevented, meaning that it must be ensured that cloned tags are detected as such, even if they are checked before the original copy.

Not every communication with RFID tags in the supply chain will include secure authentication, but there are situations when automated authentication can be a big benefit. Authentication will include additional communication, e.g. add costs to a transaction. These costs (e.g. more time for communication) should be only spent when necessary. E.g. automated customs control is such a situation where automatic authentication can be useful, although the process might take a bit longer than a standard inventory of all tags, the automatic proof that the tags and objects are genuine can help a customs officer to process the customs control faster.

3 Technology cut

This section attempts to describe how the security requirements described in the Case Studies relate to the technical tasks within the Work Package. The previous case studies have collectively demonstrated the potential economic benefits of not only RFID and EPC technology, but of the strong need for secure RFID and EPC technologies. The recurring security issues from these case studies primarily concern the maintenance of RFID and EPC system integrity, and its information confidentiality.

The technical tasks within WP4 are strongly focused upon addressing these security requirements. The work is especially focused on developing innovative solutions to these issues, rather than necessarily comprehensively documenting all the known mechanisms to help achieve this. The technical tasks are largely defined according to the 'level' in the EPCglobal Architecture on which they focus (the first WP4 Deliverable: D4.1.1 Security Analysis also analyses the system's security requirements using this layered classification).

- Task 4.2 focuses on the crypto-primitives inherent in the tag itself.
- Task 4.4 focuses on the development of a trusted secure RFID reader
- Task 4.5 and 4.6 focus on the creation of network-level security services to support confidentiality and integrity respectively.
- Task 4.3 provides an application-level security solution based upon the integration of the mechanisms developed in Tasks 4.2 and 4.4.

These innovations often combine with established security mechanisms in order to provide comprehensive security solutions that meet the needs previously described in the Case Studies. For example:

- Secure RFID tags, when combined with a network-based Authentication Service, can enable improved anti-counterfeiting and consumer privacy (Case Studies 4 and 5)
- Secure RFID tags and network-level security mechanisms combine to facilitate the reliable operation of RFID applications whose outputs can be relied upon for critical business purposes (Case Studies 1 and 3)
- The network-level security mechanisms facilitate the practical operation of Discovery Services (Case Study 2) and of all the other necessary information-sharing network elements (EPCIS's, Network Services, and potentially ONS).

Without this array of mechanisms, the majority of the benefits of the EPCglobal network would surely not be realised.

4 Conclusions

We showed that the role of security in RFID solutions is very important. Examples showed that there are huge business benefits that cannot be leveraged today because of a lack of security mechanisms. Secure RFID solutions do not just fix problems induced by RFID technology itself, but are *absolutely essential* in order to facilitate the sort of open-loop, cross supply chain applications primarily envisaged by the EPCglobal Network.

In addition to the comprehensive description of security requirements provided in the previous report D-4.1.1 Security Requirements Analysis [6], we have showed in Section 3 how these key requirements map to the actual technical work being carried out within the rest of the work package. The need and benefits of implementing security and multiple different levels within the EPC Network has also been described.

Furthermore, we acknowledge that for a wide-spread adoption of RFID, privacy and data protection standards will be a key issue.

5 References

[1] H. L. Lee, and O. Ozer, “Unlocking the value of RFID,” Graduate School of Business, Stanford University, working paper, 2005,

[2] F. Thiesse, and F. Michahelles, “An overview of EPC technology,” Sensor Review, 26, 2006, Emerald Group Publishing Limited,

[3] Garfinkel, S. L., Juels, A., and Pappu, R. (2005). RFID privacy: an overview of problems and proposed solutions. Security & Privacy Magazine, IEEE Security & Privacy Magazine, IEEE, 3(3), 34-43.

[4] L. A. Lefebvre, E. Lefebvre, Y. Bendavid, S. F. Wamba, and H. Boeck, “RFID as an Enabler of B-to-B e-Commerce and Its Impact on Business Processes: A Pilot Study of a Supply Chain in the Retail Industry,” 2006,

[5] N. Robinson, and L. Valeri, “On the Security Implications of Disruptive Technologies,” Critical Infrastructure Protection, 2007, pp. 3-14.

[6] M. Aigner, T. Burbridge, A. Dada, J. Farr, A. Ilic, and A. Soppera, “D-4.1.1: Security Analysis,” Building Radio Frequency IDentification for the Global Environment (BRIDGE), 2007.

[7] A. Ilic, T. Burbridge, A. Soppera, and F. Michahelles, “D-4.1.2: A Threat Model Analysis of EPC-based Information Sharing Networks,” ed., Building Radio Frequency IDentification for the Global Environment (BRIDGE), 2007.

[8] “Curbing Counterfeit Drugs,” 2006, U.S. Food and Drug Administration,