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

White Paper

RFID Tag Security

Authors: Manfred Aigner (TU Graz), Trevor Burbridge (BT Research), Alexander Ilic (ETH Zurich), David Lyon (GS1-UK), Andrea Soppera (BT Research), Mikko Lehtonen (ETH Zurich)

PREFACE

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

CONTENTS

1. Executive Summary

RFID is a technology that offers huge potential for change management activities by automating processes and providing accurate, trusted data. Its unique features include giving each physical object a globally unique digital identity read from a distance without requiring line-of-sight capability, and often without using a battery. These features provide new ways of measuring and integrating the real world into information systems and means RFID offers significant potential to change the way we do business. However, for RFID to reach its potential, greater attention must be paid to its security, which is the role of this work group, The Security Research Group (SRG)

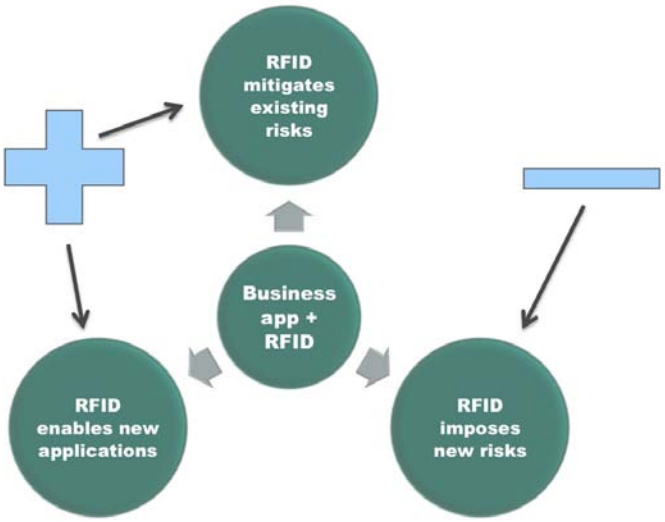

Figure 1: SRG tries to improve the balance between risks and benefits of RFID-based business applications by developing secure RFID solutions

There are three important security scenarios to consider. Firstly, when RFID is implemented to improve an existing business process, it can automate activities and thereby reduce the potential business and security risks caused by human error. Secondly, RFID itself can induce new risks to a process; mostly unlike barcodes, RFID tags will be used in security-sensitive applications such as ticketing, access control and product authentication. Therefore security is needed to keep automated aspects and invisible properties under control, and prevent any risk of the process becoming susceptible to mass abuse. Owing to the high level of automation that RFID provides, a security incident could cause great harm before countermeasures will be effective. Thirdly, as RFID is a data gathering and process measurement technology, it can completely enable new business applications. Activities and actions unable to previously be accurately measured can now deliver effective metrics. Again, security plays a major role delivering the accountability required to engender trust in the data and activities provided by these applications. These three effects are summed up in **Figure 1**.

From the SRG's perspective, we must provide security technology that supports RFID's potential in mitigating existing business and security process risks, while at the same time enabling the inherent security problems of the RFID technology to be managed. We also believe that effective security is not only a necessity for business cases where RFID improves on the existing barcode-based scenario, it also offers a completely new opportunity. Applications that cannot be deployed today because their critical points depend mainly on security will benefit from the technology we develop. Secure RFID solutions will not simply be 'must-have'; they will be an imperative enabler of powerful applications that can markedly increase organisations' competitiveness.

Usually inseparable from security issues are privacy issues, and as more businesses begin to rely on EPC-based events to manage and to share critical supply chain processes, effective solutions investigated by the BRIDGE project through the SRG must 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

With this in mind, one of the key successes of the SRG is the pioneering work done to satisfy privacy requirements through 'stunning' the tag as it leaves the store so that it cannot be read outside the store but can be reactivated when the item and tag return to that store/retailer. This means that the consumer's privacy is protected and one of retail's major headaches of reverse logistics and returns can be helped as well.

Although there have been some concerns that the strength of the password is weak and vulnerable to eavesdropping, the use of cryptographically secure tags can overcome this by implementing a secure deactivation/re-activation custom command. In addition the provision of cryptographic functions on the tag can also allow the re-activation of the tag without prior knowledge of the tag identity. This can be done by structuring a series of challenges to the activating reader that become more and more specific to the individual tag. These developments are an important and lasting outcome of the SRG work.

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 their own facilities, but also provided via unrelated third parties. The prevalence of low-cost 'track and trace' data gathering technologies such as RFID is now driving the development of global standards for the sharing of operational data traces.

The not-for-profit organisation EPCglobal has already developed a number of important standards (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 EPC Network Architectural Framework to enable the seamless gathering, filtering, and sharing of 'track and trace' data on a global scale.

EPCglobal's 1400 member companies, which work together via 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, comprise a balanced mixture of solution providers and end-users. These include Wal-Mart, Nestle, Carrefour, Metro, GE, Pfizer, and Procter & Gamble. With the recently standardised EPC Information Services (EPCIS), EPC based information sharing networks have the potential to revolutionise 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 potential application areas are not limited to *intra*-organisational closed-loop scenarios, but also to *inter*-organisational open-loop processes.

Such open-loop RFID processes support applications where items equipped with RFID tags are not limited to a predetermined set of business partners and where the assumption is that tagged items are unlikely to return to their originator (unless it is for end-of-life processes). Hence, open standards are required to enable seamless data exchange among participants.

As more businesses begin to rely on EPC-based events to manage and to share critical supply chain processes, effective security solutions investigated by the BRIDGE project through the SRG must 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.

In this whitepaper, we have shown that the role of security in RFID solutions is critically important.

There are huge business benefits that cannot be leveraged today because of a lack of effective security mechanisms. Secure RFID solutions must not just ‘fix’ problems induced by RFID technology itself, but also facilitate trust in the sort of open-loop, cross supply chain applications primarily envisaged by the EPCglobal Network. We have shown how these key requirements map to the actual technical work being carried out within the rest of the work package. The needs and benefits of implementing security and multiple different levels within the EPC Network have also been described.

Furthermore, we acknowledge that at this stage, many of the future applications which require security are not yet known, so we must avoid tailoring security requirements for a specific application. Future RFID systems planned as open loop systems will require access for many different parties and such systems must necessarily be built on standards easily accessible for any party.

2. Introduction

2.1 The BRIDGE project

BRIDGE stands for “Building Radio Frequency IDentification Solutions for the Global Environment”. The project’s objective is to enable the mass adoption of RFID for all European companies by researching, developing and implementing solutions and removing barriers to development.

2.2 Objectives of the SRG

The SRG is focused on RFID security. This means balancing the needs of applications for visibility of RFID and related data against requirements for the confidentiality, authenticity and integrity of information. Since critical business decisions are made as a result of RFID data, the integrity of the data flow is also of utmost importance. Many previous deployments of RFID have looked within a single organisation or a tightly controlled federation of companies. BRIDGE aims to remove the barriers to the global deployment of RFID and the widespread sharing of tags and information between dynamically coupled organisations. The SRG aims to take down these security-related barriers by applying appropriate controls to the flow of information and trust in the data that is received from external parties. It is clear that the value of new collaborative applications of RFID will not be realised within Europe until these barriers are overcome.

The RFID security work package is primarily based on the EPCglobal architecture, although it is not restricted solely to use of this technology. The scope of the SRG work is therefore concentrated on extending the EPCglobal architecture components to meet the needs of future RFID services. Due to limited resources, we have focused the work on two areas: the tag and reader hardware; and the inter-organisation network.

Secure tags are essential for new applications that require (i) confidentiality of tag information, (ii) rely on the integrity of tag information (e.g. maintenance records), or (iii) require authentication of the tag (e.g. to stop the proliferation of counterfeit goods). the SRG believes that the use of widely-adopted standard data security methods such as the Advanced Encryption Standard (AES) can now be implemented on low-cost passive tags. Technologies that enhance privacy can also be built over this secure tag base.

While significant work has been focused on the data protection and privacy aspects of RFID, the protection of business intelligence and integrity of RFID systems has suffered a comparative lack of attention. This is a significant barrier to the success of RFID deployment throughout Europe and a major risk to early adopters of RFID, and needs to be addressed as soon as possible. Focusing on the business requirements for security will certainly stimulate and develop RFID security development, which in turn will enable further solutions to be built to address data protection and privacy issues.

2.3 Scope of the SRG tasks

We have developed the requirements for both RFID users and for what we consider to be realistic future RFID scenarios. Since security measures inevitably add significant costs to a system, the open market typically does not call for countermeasures before and until there have been successful attacks resulting in significant loss. However, in the case of collaborative RFID supply chains, we believe that such systems will simply not develop unless there is adequate security in place. We believe 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 SRG has considered these issues when targeting areas of security research and has chosen to focus its attention on new security capabilities for tags and readers to solve future application requirements, together with a significant involvement in the developing area of global RFID networks. Where possible, we use existing technology and standards to combine

our efforts with the wider security community, providing confidence in open security standards, and allowing interoperability with non-RFID systems.

2.4 Schedule of Tasks

2.4.1 Security Analysis and Requirements

The objective was to identify the economic benefits of enhanced security for RFID solutions. Effective security for RFID tags will enable firms to improve supply chain visibility and to manage and control the data exchanged. It also enables companies to manage the risks associated with RFID in privacy and personal information.

2.4.2 RFID Tag Security

The goal of this task is to develop measures for low cost tags and RFID readers to provide protection of the tag-to-reader link against identified threats. Effective security measures are based on standardised solutions using state-of-the-art cryptography to enable authentication, anti-eavesdropping, anti-tracing and data integrity. Solutions will be presented that allow integration of standardised cryptographic functionality on low cost RFID tags. Semi-passive RFID tag prototypes that are fully compatible with EPC Gen 2 serve as a proof of concept, and the RF protocol is extended by a security layer to enable access to the tag's security features. Investigations on implementation attacks are additionally performed to assess the risk of such attacks and the necessity for the development of countermeasures.

2.4.3 Anti-cloning of RFID Tags

The aim here is to build a demonstrator system that provides a defence against cloning based on the tag's authentication functionality. Using the semi-passive tag prototype, a simple anti-cloning demonstrator has been built. Compliance with standards is of major importance. The outcome of the work package is used as working example for the process of integration of security mechanisms into future versions of existing standards such as ISO-18000.

2.4.4 Development of an RFID Trusted Reader

This objective is about designing and developing a secure RFID reader compatible with the current EPC Gen 2 standard. This is important because the reader is the first device connected to an organisation's internal network and forms a key security barrier. It is also essential in operating many of the tag security schemes proposed in a scalable manner without recourse to a centralised key server for every tag read.

2.4.5 Supply Chain Integrity

This task is to develop mechanisms to detect anomalies, both in supply-chain *information* e.g. false events that are injected into or omitted from the system with malicious intent; and in supply-chain *processes* e.g., product theft and the presence of multiple tags with identical EPCs (which may indicate cloned tags) in order to preserve the integrity of the supply chain operations. The basic idea to detect information and process anomalies is to correlate multiple events (e.g. of the same product trace) in order to analyse them for inconsistencies. For example, if the same EPC is reported in different locations within an unrealistic time-frame with respect to the maximum expected speed of the product, this may indicate a cloned tag. The focus lies on detecting "where" in a supply chain anomalies occur in order to support managers in directing their security investments to improve logistics integrity.

3. Security Case Studies

3.1 Authentication

With today's widely available manufacturing technology, it is relatively easy to produce high volumes of counterfeit products that have adequate visual quality to fool both unaware consumers and even distributors of the genuine products. It is expensive, however, to establish supply chains and distribution channels for the counterfeit products and generate trust with the trading partners. Since most products flow anonymously today, it is possible for the counterfeit players to abuse the distribution channels of the legitimate products and inject their counterfeit products among the genuine ones.

Today, the problem of counterfeit trade is mostly addressed by legal countermeasures. Legal trials, however, might not be scalable enough to solve the problem since the number of counterfeit players means they are unlikely to be discovered because they cover up their activities. Counterfeit players are not always prosecuted due to the lack of effective law enforcement in their countries of origin and the fines for illicit trade are often small compared with the financial benefits obtained. These legal shortcomings mean we want to solve the problem at source by giving each product a name (identifier) and by verifying this name (authentication) while the products flow in their legitimate distribution channels. This countermeasure protects the consumers and end-users of genuine products from mistakenly consuming counterfeit products by increasing the supply chain security. It can potentially destroy counterfeiters' business case by increasing their risks and lowering their expected results, thus discouraging illicit players in general from engaging in product counterfeiting.

Product authentication is the core service that technical anti-counterfeiting countermeasures rely on. We can formulate product authentication as identification of the product followed by verification of the claimed identity. While product authentication alone, however, is insufficient to fight illegal trade, it should still be used in a business context. Ultimately, however, an effective anti-counterfeiting strategy must consist of a combination of countermeasures.

In the following we will study the benefits of RFID and the 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.

Offline - i.e. without network access - checks for authenticity can offer added value for the customer. Where symmetric cryptography is available on the tag, the verifier needs access to the key, or to a service that provides a "valid" challenge-response pair. In computer security, challenge-response authentication is a family of protocols in which one party (the verifier) presents a question ("challenge") and another party (the one who wants to prove his claimed identity) must provide a valid answer ("response") in order to be authenticated.

It is important to note that such checks must be secured against attacks, since a successful check for authentication may justify a higher price for an object. In other words, you might be willing to pay more money for your medicine, for example, if you can be sure that the product is exactly what it claims to be. So, a negative check for an original product is potentially damaging. It is not enough for many applications that cloned tags in supply chains are detectable, but it is important that clones are prevented. The consumers themselves might want to carry out their own checks for their own peace of mind. Not every communication with RFID tags in the supply chain will necessarily include secure authentication, but there are situations when automated authentication can be a big benefit.

Authentication will usually include additional communications and therefore will add costs to a transaction. These costs (e.g. more time for communication) should only be incurred where necessary. Automated Customs control is an example where automatic authentication can be useful, and although the process might take a little longer than a standard inventory of all tags, the automatic proof that the tags and objects are genuine can help a Customs officer process individuals going through the control point faster.

3.2 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' compound as the consignment moves along the process between players, providing a fully certified audit trail of the consignment's activities, and offering the end user proof of the consignment's authenticity on arrival at its final destination.

In November 2006 the European Federation of Pharmaceutical Industries Associations (EFPIA) promoted the introduction of two-dimensional barcodes that uniquely identify single packages. For its part, 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 that RFID enables, operational processes throughout the supply-chain can be monitored more frequently. Consequently, it can provide a more detailed audit trail that results in a higher level of protection against the 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) recommending RFID technology for the implementation of e-pedigree solutions.

3.3 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 that check activities against pre-set parameters, significantly adds to the service quality of such a system. In addition, the removal of a 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 the 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 the 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 lacks trust, and consequently has no value.

3.4 Reusable Transport Items (RTIs)

The movement of many of the above mentioned products through a logistical supply chain is frequently dependent on the use of Reusable Transport Items (RTIs) – such as crates or pallets - as the medium for their transportation. From a cost perspective, tagging an RTI is particularly appealing as the costs of RFID tags (and any additional sensors) amortise over its long lifetime. The 'movement' of the RTI is how the transport of the consignment's products is managed i.e. via 'association' (as opposed to monitoring the movement of the actual products themselves). As the RTI is the carrier on which the movement of product is based, it is

imperative that the progression, location and organisation responsible at any particular point in time for the RTI is known. This ensures that assets are used efficiently and that any responsibility for damage, loss, delay etc. which will affect the business can be accurately determined. The units themselves have an intrinsic value which when lost or misdirected, will need to be replaced at a cost to the business. The user and process players will only accept such a system if all data on which the system is making process-related decisions, together with any business-related information provided by the system, can be trusted to be a true and accurate reflection of the actual situation. 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, add data, or use data to undertake 'data mining'-based analysis of activities that results in economic or business loss to end users and other parties.

3.5 Enabling After-Sales and Returns Whilst Protecting Consumer Privacy

A problem facing the world of RFID today is how to balance the requirements of consumers for privacy against the need to operate efficient and secure return processes. If the RFID tag is removed or permanently disabled, then other means such as a receipt must be used to serially identify the item. Such receipts are often misplaced, and may also be used to return similar items to the one described by the receipt. The returns process can thus be subverted to return a faulty item purchased from another shop, or claim an expired warranty on an item (by presenting the receipt of a more recent purchase).

Many potential solutions to this problem are being considered by the industry, such as moving the EPC number into reserved memory which may be protected by a password, or placing the tag into a 'stunned' or quiet mode. The problem with such approaches is that:

- The strength of the password is weak and vulnerable to eavesdropping
- The identification of the tag must still be recorded somewhere (such as the receipt) to enable the re-activation of the tag for reverse supply chain purposes.

The use of cryptographically secure tags can overcome this first problem by implementing a secure deactivation/re-activation custom command. In addition the provision of cryptographic functions on the tag can also allow the re-activation of the tag without prior knowledge of the tag identity. This can be done by structuring a series of challenges to the activating reader that become more and more specific to the individual tag.

Cryptographically secure tags will have an increased cost above insecure or password protected tags. However in some cases (e.g. for subversion of returns processes for high value goods) they may be warranted today. In cases where cheaper deployments are taken for today's processes it is important that the solution can be migrated to higher security protection as the threat evolves and is re-assessed. Thus, it is important that security features comply with standards such as EPC Gen 2 and that secure tags can operate in parallel with insecure or password protected tags.

4. The Background to RFID Security

4.1 Tag and System Security

It is important to explain how the security requirements described in the case studies relate to the technical tasks within the work package. Previous case studies have collectively demonstrated the potential economic benefits of not only RFID and EPC technology, but of the strong need that those technologies be secured. The recurring security issues from these case studies primarily concern the maintenance of RFID and EPC system integrity, and the confidentiality of the system's information.

These innovations often combine with established security mechanisms 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 or access control service, can deliver improved anti-counterfeiting and consumer privacy and ensure integrity of the data introduced into the RFID network.

- 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
- The network-level security mechanisms facilitate the practical operation of Discovery Services and of all the other necessary information-sharing network elements (EPCIS, Network Services, and potentially the Object Naming Service (ONS)

4.2 The RFID tag industry today & its future

Given the choice of a cheap tag that costs a few cents and a secure tag, most end users will always go for the cheapest solution. However, as the number of RFID applications increase and include open loop systems with access from many parties, we can foresee that the current lack of security will be a major impediment in many solution designs. Our view is that Moore's Law - Intel co-founder Gordon Moore wrote in a 1965 article that the number of transistors on a chip would double every 24 months - and market drivers will soon enable security functionalities on low cost tags. The default choice of using cheap, unsecured tags must change if tag security can be seen to be a service-enabler and security management can be made 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, just as car-immobilisers work 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 application also determines the value to the attacker and hence the capabilities that an attacker will bring to breaking the system.

4.3 Current RFID security capabilities

The key advantage of RFID technology over earlier technology, such as optical barcodes, includes the ability to identify objects without line of sight access. However an RFID system is more than a series of radio frequency tags. Any benefit relies on the system being capable of acquiring data from the tag and transforming that data into useful information for specific business processes.

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.

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 so do not have special requirements for protection of the information. If tags are operated as a substitute for bar codes and are only used in environments that limit physical access and eavesdropping, then additional security will not bring a benefit to these applications. Within the SRG, we are trying 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, for example, the use of passwords to control the operations (for example, the writing or killing) of the tag. However, the security of such simple passwords is low because a password can easily be eavesdropped and re-used and the cost of managing these passwords is significant.

The data protection working group of the European Commission analysed RFID technology identifying 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) they state that when RFID tags contain personal data, they must provide technical measures to protect this data from unauthorised 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"*.

4.4 Transponder ID (TID) Numbers

Like most RFID tags, EPC tags store Transponder ID (TID) numbers that identify the chip's model and manufacturer. These numbers are written on the chips during fabrication and they are protected against rewriting. A TID number can optionally include a serial part that also identifies the unique chip. These serialized TID numbers are written on some existing Gen-2 chips and are expected to become a common feature of Gen-2 chips in the future.

On the one hand, serialised TID numbers can be a big headache for RFID hackers who want to clone tags. While a tag's object ID number, such as the EPC, can be easily changed, changing the write protected TID number is considerably harder. As a result, chip manufacturers advertise the serialised TID numbers as security features of Gen-2 chips. On the other hand, the use of serialised TID numbers as security features represents a big opportunity for RFID hackers. In contrast to cryptographic tags, serialised TID numbers do not provide any real security against tag cloning. For instance, there is nothing that prevents an adversary from reading the serialised TID number of a tag and transmitting this number to a reader to impersonate the tag. In addition, if chips with programmable TID numbers became commercially available, cloning serialised TID numbers would become as easy as cloning EPC numbers.

Despite these obvious vulnerabilities of the TID scheme, it would be incorrect to claim that serialised TID numbers do not provide any security against tag cloning and impersonation; since RFID tags with programmable TID numbers are not available in the market today, it is currently not easy for an adversary to produce an RFID tag with a copied serialised TID number.

TID numbers begin with an 8-bit ISO/IEC 15963 Allocation-Class (AC) identifier [3]. The ISO/IEC 15963 standard describes the mechanism to guarantee uniqueness of the TID numbers and presently four organisations have been assigned an AC identifier [1]. The allocation-class identifier for EPCglobal is $11100010_2 = E2_h$.[1] For tags whose AC identifier is $E2_h$, the EPC Gen-2 standard requires that the TID memory be comprised of a 12-bit Tag Mask-Designer Identifier (Tag MDID) and a 12-bit Tag Model Number. According to the Gen-2 air interface specification [2], the TID memory may also contain tag and vendor-specific

[1] 1Subscripts 2 and h stand for binary and base-16 (hexadecimal) number formats, respectively

data such as the serial number. The content of the TID memory bank defined by existing EPC standards is illustrated in Fig. 1.

TID MEM BANK BIT ADDRESS	BIT ADDRESS (In Hex)															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
10_h-$1F_h$	TAG MDID (last 4-bits)				TAG MODEL NUMBER (12-bits)											
00_h-$0F_h$	11100010_2=$E2_h$								TAG MDID (first 8-bits)							

Figure 1. TID memory structure in the current EPC standards [3]

For tags whose AC identifier is $E0_h$, the ISO/IEC 15963 requires that the TID memory comprise of an 8-bit tag manufacturer ID and a 48-bit tag serial number. Furthermore, the standard requires that the TID memory be permalocked. The ISO TID structure is illustrated in Fig. 2.

TID MEM BANK BIT ADDRESS	BIT ADDRESS (In Hex)															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
30_h-$3F_h$	TAG SERIAL NUMBER (48-bits)															
20_h-$2F_h$																
10_h-$1F_h$																
00_h-$0F_h$	11100000_2=$E0_h$								TAG MANUFACTURER ID (8-bits)							

Figure 2. TID memory structure in the ISO standards [3]

The upcoming EPC Tag Data Standard is likely to make locking the TID numbers mandatory and define a way to specify serialised TID numbers. This is expected to be done with an extended tag identification number (XTID) that extends the current EPC TID format with an 48-bit (or more) serial number and information about key features implemented by the tag. Though chip manufacturers can still opt for a non-serialised version of the TID within this scheme, the new standard is presumed to foster the adoption of serialized TID numbers.

One way to clone the serialised TID numbers, in theory, is to purchase standard tags and to manipulate the content of their TID memory. Even though standard tags' TID memory is write-protected, there are ways to bypass this protection using special equipment like a Focused Ion Beam (FIB). However, these kinds of attacks are costly and labour intensive.

Another way to overcome the TID checks is to manufacture fully programmable tags. If any existing chip manufacturer would sell UHF chips with programmable (unlocked) TID memory, the security of the TID checks would be completely undermined; an adversary could simply buy an empty chip and write the wanted TID number on it. Nothing would prevent a semi-conductor foundry from manufacturing fully programmable chips and a chip manufacturer from selling them. Though producing chips is costly, this possibility needs to be considered if TID-based authenticity checks are planned to be used on a large scale basis (e.g. pharmaceutical or tobacco brand-wide).

Last, TID checks can be bypassed by building a device that effectively emulates or imitates an RFID tag, without the need for IC manufacturing. This kind of device could fool the inspections if the tag is not seen during the check. This could be done in practice, for example, when pallets or cases of goods are verified by distributors or customs and the impersonation device is hidden inside the package. In addition, in the case where the tag is not a label but a hard tag (encapsulated tag), the spoofing device could be built inside it. These kinds of encapsulated tags are used in applications requiring longer life cycle for the tag or tolerance for harsh conditions. Fig. 3 illustrates a programmable semi-passive tag prototype, developed in the BRIDGE project, and a commercial encapsulated tag.

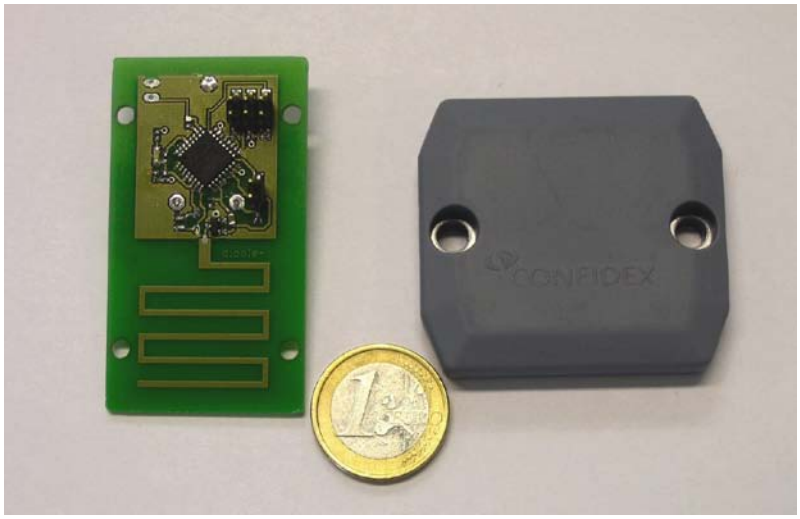

Figure 3. Programmable semi-passive tag prototype (left) and a commercial encapsulated tag (right) (courtesy of Confidex Oy)

5. RFID Tag Security measures

This work package is dedicated to the development of secure RFID tags. These include protection measures on the tag itself, but also of the wireless communication link between the tag and the reader and require the creation of technical protection measures on both tags and readers. Depending on the final application, these new measures can be used to build anti-tracing and anti-tracking mechanisms for RFID technology or to provide secure authentication of the tags. The aim of the project is to provide suggestions and a proof of concept for successful implementation of cryptographic protection that can be applied in open loop RFID systems and that comply with the restricted computing resources of low-cost RFID tags.

The suggested security measures are based on a symmetric cryptographic approach, implemented in a way that the reading distance of low-cost tags is not reduced. In symmetric cryptography, identical cryptographic keys are used for both decryption and encryption.

The additional cost due to the marginally increased chip area of the tag chips is justified by the additional value such protection functionality can provide. Cryptographic functionality together with proper management of secret keys can be used as so-called “privacy enhancing technology” and is suggested as such by the Article 29 data protection working party as a measure to protect “personal data” stored on the tag. Additionally such functionality can be used to provide tag and reader authentication with the capability, in principle, of providing a proof-of-origin of tags and readers. Tags which can provide such authentication facilitate anti-cloning applications, while reader authentication offers the possibility of allowing specific access to the tags’ content only for authorised readers. The suggested solution will therefore provide technical measures for RFID tags to allow compliance with data security regulations and principles and to prevent eavesdropping and cloning or the unauthorised modification of the tag’s memory.

Several related tasks tackle the problem from different perspectives:

- Development of prototyping platforms: We are developing three semi-passive tag prototypes that can be easily extended with additional functionality. These semi-passive tag prototypes are fully compatible with the EPC Generation 2 Class 1 protocol.
- RFID pseudonym scheme: Using a semi passive-prototype we can demonstrate how the basic security functionality can be used to develop a pseudonym scheme that provides protection of the tag identifier and prevents tracing of the tag history.
- Comparison of crypto primitives: Hash, encryption and stream cipher primitives are compared for incorporation into future secure tags.
- Implementation attacks: Investigation of the threat of “Side-Channel Attacks” to discover whether RFID technology is susceptible to those attacks and to what level of security the tags need to be protected.
- Key management: Investigation into the problems of storing secret keys on tags.

5.1 Physical protection of a tag

Cryptographic tokens such as 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 also store a secret key which must be protected. Smart cards and tags operate in similar environments - a completely un-trusted environment - which means that the cryptographic device is potentially under the full control of the potential attacker. Attackers can easily get their hands on tags and 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.

It is important to realise that attackers can use and destroy tags to get information about others. Since tags are available for a very cheap price in seemingly unlimited quantity, an attacker can operate tags beyond their specified operating conditions range and try to find vulnerabilities under special circumstances.

5.2 RFID Tag Security Requirements (Required Security Operations of a Tag)

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. However, not every application requires the support of all possible operations:

Authentication: (Tag authentication): The requirement for tag authentication comes typically from anti-counterfeiting applications because a tag that supports tag authentication can provide proof of its identity by cryptographic measures. Authentication is also necessary for applications that require anti-eavesdropping measures, since successful authentication is a prerequisite for encrypted communications, otherwise an attacker could easily request information under the faked name of an authorised party. Without prior authentication, the victim of such an attack would send the information although perfectly encrypted, directly to the attacker.

Reader authentication: 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 reader's authenticity 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. Cryptographic capabilities on the tag are required to deny access to unauthorised readers and/or to encrypt the tag information during communication

Signature: RFID applications may require signature functionality for tags. i.e. a reader can request that a tag signs information sent to it. By utilising this signature, any other party can prove that a specific tag has originated the communication. A typical scenario might involve the concept of pedigree where a party other than the reader needs to trust that a security tag was read. For pharmaceuticals, being able to authenticate the tag is a critical part of providing e-pedigree. Sharing, or validating this data at every step throughout the supply chain is key to any e-pedigree program.

6. RFID Security and Privacy

6.1 Privacy risks

In the last few years, the availability of RFID technology has raised a number of privacy concerns and organisations that implement RFID solutions need to prevent the technology from infringing the privacy of the consumer. Experts participating in the BRIDGE interview process have identified that even if the actual privacy threats of RFID technology are low, there is a significant risk that the perception of a threat to their privacy by end-users can lead to a serious undermining in the company's image and reputation with its customers.

In order to safeguard consumer privacy we could include cryptographic algorithms in the tag. However, the main challenge is the cost of such tags. Yet, 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." The technical challenge here revolves around how we should enforce such a policy and much more needs to be done in this area.

6.2 Data Protection

The SRG Security work package is concerned with developing effective research and technical solutions for RFID security. This 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.

So, it is necessary to discuss 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'. 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.

6.2.1 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 undertaken 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 and the SRG has developed 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 that have stronger security requirements, the secrets may only be released through 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 SRG's work on the development of a Trusted RFID Reader provides an alternative to tag access control. Using the Trusted Reader, permitted read policies can be enforced.

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 can also be easily withdrawn from the reader without requiring the writing of new secrets onto the RFID tag.

The SRG is also concerned with the integrity and confidentiality of data exchanged over the network from RFID information systems and applications. Techniques to control the spread of sensitive business information also cover 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 because 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.

6.2.2 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 work package as it deals with data quality and retention. RFID systems should always be managed along with other information systems within a business to meet the appropriate and where necessary, legal, requirements for data protection and privacy.

6.2.3 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 except: a) with the consent of the data subject; or b) by the authority of law."

Before any data is passed to the next onward component in an RFID system, the identity and intention of the onward party should be made 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 ongoing 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 a release should only occur once the identity of the system is known and appropriate credentials have been 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. Standards Compliance and Evolution

The current EPC Gen 2 or ISO 18000-6 C allow for the provision of custom commands which can be used to implement secure protocol commands such as tag authentication, or access controlled memory. This means that tags providing such security functionality can operate alongside today's insecure RFID tags using the same reader infrastructure and comply fully with the use of such standards.

Early deployments of tags with secure functionality (e.g. authentication command) are likely to be in limited environments. Thus potential readers will be able to recognise which tags have additional custom security commands from the Tag Identifier (TID) or the EPC number. As secure tags become more pervasive the standards need to be extended to signal which capabilities (e.g. security, sensors, memory) a tag provides. This is desirable in scenarios where looking up TIDs becomes infeasible (for scalability or connectivity reasons) or where the identity of the tag must itself be protected.

Finally, extensions to the protocols may be required if a significant class of tags requires confidential identifiers. Although such schemes can be implemented as custom commands (leaving the EPC field blank), this prohibits the parallel reading of multiple confidential identifiers. To enable this, the inventory command would need to be extended to accommodate random numbers shared between the reader and the tags that can be used by the tags in the generation of seemingly random pseudonyms (instead of a constant EPC). Such random numbers are required to stop the cloning of previously observed valid tag responses, or the tracking of tags by malicious readers.

Tag Security Features

Feature	EPC Gen2	Cryptographic Tag
Confidentiality of Tag Identity	No current direct support. Can move EPC into reserved password controlled memory, and avoid tags with serialised TID. Password and ID may be subject to eavesdropping and attack on weak password. There is no way of managing which password is required to access a tag (other than recording on consumer receipt, shipping record or other associated media)	Produce pseudonym instead of static EPC
Access Control	Password control for reserved memory. Password and data may be subject to eavesdropping and attack on weak password.	Access control through knowledge of strong cryptographic key. Eavesdropping not possible.
Authentication	Reliance on publicly visible TID. Dangerous assumption that TID will not be cloned.	Authentication through cryptographic secret key held on tag. Since key is never released it is harder to clone.

8. Conclusions

Objective

The objective of this report was to review current RFID tag security activities and investigate future requirements.

Where applications require tags with security functionality, 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 building blocks and standardisation, and are therefore inappropriate for use within an open loop EPCglobal network infrastructure.

With this result in mind, the ongoing purpose and focus of the SRG activity must be to build security functionality into tags and readers to provide applications with a secure platform that can be used to implement their specific security functions and commands.

Usually inseparable from security issues are privacy issues, and as more businesses begin to rely on EPC-based events to manage and to share critical supply chain processes, effective solutions investigated by the BRIDGE project through the SRG must 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.

With this in mind, one of the key successes of the SRG is the pioneering work done to satisfy privacy requirements through ‘stunning’ the tag as it leaves the store so that it cannot be read outside the store but can be reactivated when the item and tag return to that store/retailer. This means that the consumer’s privacy is protected and one of retail’s major headaches of reverse logistics and returns can be helped as well.

Security risks that require ongoing investigation

At the tag layer, 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 compatibility with non-secure RFID reader infrastructures. (Any solution must cater for the ability for secure tags to be read by insecure readers and vice versa). In addition, the operational security requirements of the tag should be considered regarding elements such as tag authentication, reader verification, confidentiality via encryption, tag signature and data access levels.

At this stage, many of the future applications of which effective security will be a prerequisite are still unknown, so we must avoid tailoring security requirements for a specific application, or indeed, thinking too rigidly about security risks. However, it is clear that future RFID systems will be planned as open loop systems, with access for many different parties. Such systems must necessarily be built on standards that are easily accessible for any party – and that are equally easily and effectively secured.

References

[1] Frmling, K., Tossavainen, T. and van Blommestein, F.: Comparison of the ID@URI (TraSer) approach with other systems. TraSer-Project White Paper (2007)
[2] EPCglobal: Class-1 Generation-2 UHF RFID Conformance Requirements. Version 1.0.2.
[3] EPCglobal: Class-1 Generation-2 UHF RFID Protocol for Communication at 860 MHZ - 960 MHz. Version 1.1.0.
[4] Lehtonen, M., Ruhanen, A., Michahelles, F., Fleisch, E.: Serialized TID Numbers – A Headache or a Blessing for RFID Crackers? In the IEEE RFID 2009 Conference, Orlando, Florida, April 2009.[2]

APPENDIX 1

An Introduction to RFID Technology

RFID Journal magazine defines an RFID tag as *"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."*

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 a farm-animal), buttons and low cost label-type packages. The most important focus for the SRG 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. In UHF technology especially, tag-antenna design is crucial for the reading range that can be achieved.

- Silicon: A small silicon chip that includes all the electronic circuitry delivering the functionality of the tag. The on-chip electronic circuitry can again be divided into three separate subsystems:

Receiver/Transmitter (or the 'analogue part'): This part of the electronic circuit is responsible for reception and transmission of the analogue EM-signals and transforms them into a power supply and digital signals for furthercomputation on the tag.

- Digital circuitry: This element 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: 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 also 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.

The SRG has focused its activities 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 the SRG, 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 (i.e. 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 crucial. Contact-less smart cards are used in applications with high security requirements, and justify a completely different market price segment.

Thus, the functionality of RFID tags should be limited to the absolutely necessary features needed to keep costs to 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 metre 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 of a typical CL-smart card.