Project IST-034144: SToP
Stop Tampering of Products

Deliverable 4.2

Analysis, Design, And Preparation Of Production, Assembling And Training Processes For The Production Of Smart And Verifiable Products Using RFID

Leading Partner: SPC

Security Classification: Public (PU)

May 2008
June 2009 (update)

Version 1.1

Project Details

IST Project Number	034144
Acronym	SToP
Project Title	Stop Tampering of Products
Project URL	http://www.ist-stop.eu/
EU Project Officer	Peter Friess

Authors (Partner)	Craig Cook (SPC), Harald Vogt (SAP)		
Responsible Author (Partner)	Eric Gout (SPC)	**E-mail**	eric.gout@spacecode-rfid.com
		Phone	+33 1 69 75 21 73
Peer Reviewer	Thorsten Staake (ETH)	**E-mail**	tstaake@ethz.ch
Final Approval	Harald Vogt (SAP)	**E-mail**	harald.vogt@sap.com

Version History

Version	Date	Description	Comments
0.5	08-02-21	Initial	Created (EG)
0.9	08-04-15	Complete	All comments included (TS)
1.0	08-05-27	Final	Review and finishing (HV)
1.1	09-06-22	Final	Blister pack include (EG)

Table of Contents

Table of Figures

Table of Tables

Executive Summary

The mission of SToP is to develop secure, comprehensive, usable, cost effective and convenient product authentication mechanisms to reduce the trade of illicit products. The project's main objective is to develop a distributed, collaborative, ambient and intelligence-based network-oriented system which will enable enterprises, including producers and distributors, as well as customers to manufacture, deliver and purchase authentic products.

SToP is developing solutions which go beyond the current state-of-the-art Radio Frequencey Identification (RFID) based anti-counterfeiting methodologies. Inherent in any novel state-of-the-art technology is uncertainty and lack of experience regarding selection of an appropriate technology, implementation, successful deployment and scale-up. The key to success is to understand the technology, its advantages, and the challenges – and then synthesise this into a well researched preparation and execution plan with all the required detail. Deliverable 4.2 focuses on the analysis to identify and select the optimal RFID technology and approach. It outlines the process followed in SToP to select technologies for end user partners (to be trialled in the WP5 pilots). It considers what needs to be taken into account prior to the implementation of a new smart/verifiable solutions that will be integrated into products during their production lifecycle.

Thus the approach used provides a framework of implementation considerations and challenges for successful integration and deployment of the novel RFID solutions to achieve the consortium's anti-counterfeiting objectives, which then feed into the next stages of the work package where real life deployment of the solutions occur.

Given the recommendations of D4.1 and the requirements of end users, this report will focus primarily on using RFID as the cornerstone technology of this next generation solution and its integration and deployment. The information and recommendations will also be relevant and applicable to other technologies and approaches identified in D4.2.

1 Introduction

1.1 Project Description

SToP is an EU subsidised project developing an anti-counterfeiting solution for companies concerned with or affected by fake products, including luxury goods companies, pharmaceutical companies, and aviation companies.

This solution will comprise the evaluation and development of advanced smart identification technologies (such as RFID, and other technologies) together with the design of suitable and scalable software and architecture components as part of a comprehensive secure network infrastructure. The project, development, and final solution will be driven by the requirements of the end users within the project consortium.

The financial support of the EU for the project is testament to the importance and urgency it attaches to achieving success in its fight against counterfeiting. The consortium of companies comprises leading technology vendors and end user companies, as well as academic institutions committed to achieve the objectives of developing a sound anti-counterfeiting solution for use in the European Union and, by natural extension, globally.

SToP recognises the key and central role of companies in the anti-counterfeiting initiative, and ultimately that for the solution to be feasible and successful it needs to satisfy the diverse business sector requirements and make also economical sense. Legitimate businesses bear the brunt of counterfeiters' operations, and it is the dedicated intention of SToP to eliminate as far as possible counterfeiting and its adverse consequences on the companies' sales, market share, revenue, operating profit, litigation costs, and working capital. Moreover reducing or eliminating fake goods ensures that the brand is not eroded and confused with counterfeit copies, and company reputation is maintained and enhanced. For society, the most important benefit is product safety - counterfeiters do not respect quality standards to ensure user safety or benefits. Bogus products such as pharmaceuticals, aviation spare parts, toys, etc can be potentially dangerous or even lethal. There have been numerous cases worldwide where counterfeiting of products resulted in serious, life-threatening or even fatal results for the consumer.

SToP deliverables will enable immediate implementation and integration into the particular companies' product portfolio and offerings - luxury goods, pharmaceuticals, security documents, aviation components, etc - and the related manufacturing and packaging as well as inventory control and logistics processes, to eliminate counterfeiting and its consequences for the respective companies and their customers and partners; as well as national authorities. For the EU the project is seen as a cornerstone initiative and deliverable in its fight against illicit trade.

1.2 Objective of Deliverable 4.2

Deliverable 4.2 is the second report generated in Workpackage 4 which relates to Solution Engineering and hardware research and development to achieve SToP anti-counterfeiting objectives.

This document addresses the preparation for implementation and deployment of RFID based anti-counterfeiting solutions (including impacts, challenges, and considerations for selection, production, assembling, and business processes). Detailed analysis is provided regarding selection of the technology/technologies for the SToP consortium, and the process followed. As with any novel state-of-the-art technology project there can be a certain amount of anxiety due to the unfamiliarity of the technology and the approach. The paper is written to address any uncertainties and provide clear directives on what is required for, and what to look for in, deploying such a technology.

The results of this task will provide important information for the real-world evaluation of the concepts.

1.3 Relation to Tasks, Deliverables and Workpackages

Workpackage 4: This deliverable follows on from, and is linked to, deliverable 4.1. Deliverable 4.1 created the foundation for all subsequent work carried out in work package 4 by researching and analysing existing smart/intelligent devices that are conformant to the requirements of SToP. Deliverable 4.1 scrutinized existing and emerging anti-counterfeiting technologies, their relevance and applicability to consortium companies and industries, and proposed potential approaches to implementation as stand alone or combination technologies. The most promising approaches from a SToP perspective include RFID - with or without other laser, digital and/or printing technologies. Deliverable 4.2 builds on this, and goes into detail regarding the identification and analysis for selection, deployment and implementation of RFID solutions for consortium end users; also preparing for WP 5 where the practical applicability of RFID (already selected via Task 4.1) will be evaluated by integrating them into real life products. Tasks 4.3 and 4.4 relate more to the production and manufacturing of the smart enabled final product with integration of the respective selected technologies. Task 4.5 completes the workpackage by covering the system integration requirements, for both the hardware and software integration aspects of the anti-counterfeiting systems.

Other Workpackages: From a project process perspective, the outputs of 4.2 will be used for the next stages of the project where the RFID devices and systems will be:

- incorporated within real life products and systems (WP 4 and 5)
- integrated with the SToP infrastructure for product-authentication (WP 3, 4, 5)

Thereafter, the outputs of this deliverable will be reviewed with real life implementation experience and learnings to provide final recommendations for D4.4, *Revised analysis and design document for production, assembling and training processes for the production of smart and verifiable product*, where the focus will be on the development of corresponding real-world production and assembling processes, and also the extensions on affected machines to produce smart and verifiable products e.g. ‘smart’ watches, spare parts, and pharmaceuticals.

In addition, deliverables 4.1 and 4.2 are integral to deliverables 3.1 and 3.2, which focus on software related research. The main software deliverable is the Product Verification System (PVI) which will provide mobile and stand-alone applications and devices with the proper services and related data to easily verify the authenticity of products. Workpackage 3 approaches authentication solutions from a software and architecture perspective, while Workpackage 4 approaches it from a hardware and physical perspective.

1.4 Document Structure

The paper commences with a comprehensive discussion regarding what needs to be considered when selecting an RFID technology for deployment. There is special consideration given to both the adoption of RFID technology as well as its deployment. Using this as a framework, a detailed RFID technical analysis and evaluation is undertaken for the SToP consortium end users and their respective industries. The paper ends with a glimpse of the near-term future of RFID and our concluding thoughts on RFID and its deployment for SToP industries and companies.

Due to the inherent limitation of experience, and thus information, regarding the deployment of such novel RFID technologies, information for this deliverable has been researched from a broad arrangement of sources including semi structured interviews, the experience of project partners, web research and publications.

The intent of the document is to provide a structured perspective of the methodology used in the SToP consortium, that will be tested and fine tuned by the SToP consortium, and that can be ultimately applied and utilized externally in the industries and services represented by SToP participants.

2 RFID General Considerations

A brief overview of RFID is provided in Appendix 1; for a more detailed description the reader is referred to the vast literature available on the subject.

The key to success with RFID is to understand the technology, its advantages, and the challenges – and then synthesise this into a well researched and detailed selection, preparation and execution plan.

Radio frequency identification is a complex technology. Making it work for businesses requires careful planning and a pragmatic approach to technology identification and business case development. For SToP consortium members, particular factors need to be addressed to provide a viable, economical and secure anti-counterfeiting solution including technology selection, business case, preparation, deployment and integration, scalability etc.

In spite of increased pressure for its implementation, RFID technology is not well understood by either companies or consumers [VIS06]. It is a complex system technology that has to be precisely tailored to each application and that offers a broad range of implementation options. The increased popularity of RFID technology coupled with the lack of understanding creates a dilemma that requires careful preparation to ensure successful implementation in practice. Selection of the correct option needs to be planned according to a number of variables, and cost concerns should not overshadow more important issues in RFID implementation as outlined in this document - proper commitment, planning and partnering is required for all aspects of the project.

2.1 Consideration #1: Performance Requirements

In considering performance specifications, a company may need to consider a number of trade-offs between performance, cost, read range, read speed, product components such as metal, tag placement such as overt versus covert etc.

Given the different permutations of RFID solutions and frequencies, Table 1 below provides a framework of key performance indicators for RFID systems that are important for end user anti-counterfeiting applications, and benchmarks each variable as a function of available RFID frequencies.

	Passive Tag			**Active Tags**
RFID Feature	Low Frequency (LF)	High Frequency (HF)	Ultra High Frequency (UHF)	High and Ultra High Frequency
	<135kHz	13.56MHz	860 – 960 MHz	433MHz, 868MHz, 2.4GHz
Power	Magnetic > Electric	Magnetic > Electric	Electric> Electric	Battery
Global Availability	Yes	Yes	No	No
Interference by Metal	Minimal	Some	Significant	Significant
Absorption by Organic Material	None	Some	Significant	Significant
Typical Tag Size	> 0.5cm, < 10cm	> 0.5cm, < 3cm	> 7cm, < 13cm	6cm – 12cm
Reader Antenna Size	Customised	Customised	12 – 16cm	2 – 11 cm
Interface Algorithm	Any	Any	Any	Any
Impact of Item Orientation	Some	Some	Some	Some
Impact of Item Proximity	Some	Some	Significant	Some
Reading Distance	0–1.5m defined	0–1.5m defined	5m, undefined	Up to 100 m
Data Rates	~ 5 kbps	~ 20 kbps	~ 60 kbps	28- 60 kb/s
Detection Rates	10 – 40 tags/s	10 – 50 tags/s	100 – 500 tags/s	200 tags/s
Cost	+	+	±	++/+
Longevity	+++	+++	+++	+
Disposal	n/a	n/a	n/a	Batteries

Table 1 : RFID Frequencies and Trade-Offs

Tags:
RFID tags can be categorised essentially into two primary categories: active and passive tags. Active tags are more costly since they contain a battery that provides power so the tag can transmit a signal, up to 50 meters, to a reader. Passive tags do not contain a battery but instead draw their power entirely from the reader's field, thus have a shorter read range, and hence are much cheaper than active tags and therefore can be used more cost effectively to track at the item levels. Furthermore, passive tags longevity are not limited by shelf life of the batteries, and disposal of the batteries does not need to be considered. Passive tags are read when they pass through the electromagnetic field of a reader. Tags can be read only, write once/read many times or read-write. Data on a read only tag cannot be changed and they are often used to track assets that will have a unique ID over their lifetime such as for medications, luxury goods, and aircraft parts. A read-write tag will allow changes to the stored data and they are used to track items through the supply chainproviding a living history of the item being tracked RFID tags can be manufactured from a variety of proprietary or standard chip and code formats eg the Electronic Product Code (EPC) which uses a 96-bit scheme advocated by EPCglobal.

Readers:
Read range and speed of data transfer increase as frequency increases, but higher frequencies also have reflection problems and are negatively impacted by metal, liquid, glass and moist environments; and the health risk to workers is higher due to increased radiation.. Low frequencies on the other hand are not impacted by the presence of metal and can even read through some non-ferrous metals [WIDE04]. Antenna shape (reader and tag)and design also affect the RFID performance

parameters. A circular polarised reader antenna should be used if the tag orientation in the radio frequency field is unknown, while a linear polarised reader antenna provides greater radio frequency penetration and longer read ranges.

No single RFID frequency can thus ubiquitously satisfy all customer requirements. Pure physics defines differences between the various frequencies that results in different frequencies being better suited to different applications. For example UHF has a long read range and high read speed but when operating in metal or organic environments the performance reduces dramatically; LF on the other hand has a lower read range and read speed but excellent performance in the presence of metal or organic material. Differences in performance manifest as differences in read rate and accuracy.

Relevance to SToP:
RFID system performance requirements must be clearly understood and defined by companies implementing RFID. The anti-counterfeiting objectives of consortium end users are likely to be best served by passive tags. The main reasons include i) performance – ie adequate read range, read speed, and reliability; ii) integration size – ie smaller form factors since no battery attached; iii) cost – passive tags are cheaper than active tags iv) longevity – the lifespan of passive tags are not limited by battery life and v) environmental concerns – the disposal of batteries from active tags is a sensitive, time consuming and costly process. Read-write functionality may be required for the pharmaceutical and aviation companies in the consortium, while read only functionality will likely be required for the luxury goods industry.

2.2 Consideration #2: Cost

Cost is a major factor in determining whether or not RFID is adopted (due to concern that investment in RFID will not pay off), and if so the speed at which it is adopted. RFID systems require expenditure for tags, readers, hardware, software and system maintenance. Although costs continue to fall – by between 10% - 30% annually since 2001 (for example from about €1 per tag in 2000 to about €0.10 in 2003 [OCO05]) current costs for passive tags can still be anything from €0.10 to €1, and for readers from €100 to €5,000 (depending on performance requirements). Applying these costs to an enterprise rollout could result in several hundred thousand Euro's for a warehouse or distribution centre, up to fifty or one hundred thousand at store level per store; and this excludes any IT integration to integrate the RFID system into existing information systems.

Relevance to SToP:
Given the global coverage and high volumes of products shipped by the consortium companies The pharmaceutical industry, Airbus, and Richemont; tag costs will need to be maintained at acceptable levels. But as covered in Workpackage 2, costs must be considered from a total cost perspective (rather than on individual tag unit costs) and the threshold level at which positive NPV and ROI is generated. Moreover, as volumes in the market increase, companies can expect to leverage this fact to achieve substantially lower per unit costs for tags and readers.

2.3 Consideration #3: Standards

Standards can be applied to format and content of the codes on the tags, protocols and frequencies used by the tags and readers, the security and tamper-resistance of methods, network architecture, software and middleware. In the RFID market, two main RFID standardization bodies exist – EPCGlobal and ISO where a number of standards have been developed. For example, several ISO standards are now established, including ISO 11785 for 125 KHz (low frequency), ISO 15693 for 13.56MHz (mid frequency), and ISO 18000-6 for 860-930MHz (Ultra High Frequency (UHF)). Ratified standards by EPC Global include a standard for the 13.56MHz frequency (Class one) and more recently HF Gen 2 for tag protocol; while for UHF 3 standards exist - Class 0 and Class 1 – and more importantly UHF Class 1 Generation 2 (which has now also been ratified by ISO) which replaces class 0 and class 1 - have been developed and approved by EPCglobal. Theoretically to gain maximum benefit from RFID in the supply chain, various business partners worldwide need to use common tags, readers and frequencies so that they can be used beyond the confines of a company's walls. The establishment of a standard will force cost to drop as RFID product suppliers can all produce compatible chips, readers, associated hardware and software.

Besides standards, many proprietary solutions are available. Customer requirements determine whether a proprietary or standardized solution is better suited to respective environments and processes. In certain instances proprietary solutions may better provide the desired specifications for a particular customer, in other instances standardized solutions may be preferred. The existence and implementation of standardized and/or proprietary solutions are not mutually exclusive

Issues with current standards reflect the early stage of development of both the industry and standards including:

- they do not meet all customer requirements.
- item level tagging is not currently adequately addressed.
- they do not currently achieve full and reliable operation in harsh environments such as metal, organic material, liquids, close proximity, multiple orientations
- no one frequency can ubiquitously satisfy all RFID requirements.
- different frequencies have different attributes that result in certain frequencies being more appropriate than others in different environments and circumstances.

Because of this, many industries and companies require solutions now that are not technically feasible under existing standards. Thus companies need to focus in the first instance on what technology works the best in their environment, and then on whether it is a standardized or proprietary solution.

Moreover, anti-counterfeiting RFID solutions may best be served by non standard technologies to minimize the amount of information and know how that counterfeiters can access with standardized solutions.

Relevance to SToP:
Interestingly and for good reason, there are currently no specific global anti-counterfeiting standards in place or under development - representing the inherent conflict between making solutions widely available for end-users on one hand, while on the other needing to keep the solution from being exploited, undermined and breached by counterfeiters. SToP end users will need to carefully evaluate and decide if a standardized or a proprietary system would better fit their needs while considering both performance and security perspectives.

2.4 Consideration #4: Security and Privacy Risks

RFID may pose security and privacy risks to both organisations and individuals. Unprotected tags run the risk of eavesdropping, tampering, lifting, cloning, etc and data obtained from RFID tags can be misused in a variety of illegal ways including legitimising fake goods, reducing the price of expensive items, theft, corporate espionage, etc. RFID technology used at the item level can be used to obtain information about customers and to track their movement without their knowledge. Some steps to reduce the privacy concerns of consumers include for example using RFID only on pallets, cases and shelves for streamlining the inventory and supply chain handling systems, but not at the item level. If tags are used at the item level, they could be deactivated after the POS, or various PKI, encryption and access techniques can be used (and are being used) [JUE05]. Also simple but effective, is to obtain the consent of the consumer including letting them know that an RFID tag is on the product and it can be removed at checkout if the customer so desires, otherwise it can be left on the product if the customer has no objection. Similarly, if a retailer is going to use the information obtained from the tags, they need to make that information and choice available to the consumers. Next generation tags could incorporate additional blocking and encryption systems, designed to protect privacy and unauthorised reading within certain bounds eg information can be collected only to the extent permitted by law, no information could be collected before a transaction or after it was completed, etc. Also, programmable read-write tags can be encoded with security features that limit access, and to identify and record unauthorised reads.

More detailed discussions on security are provided in Deliverables 3.1 and 4.1

Relevance to SToP:
Privacy and security are main focus areas of the project specifically for consortium end-users involved in the project like the pharmaceutical industry and luxury goods companies. It could be foreseen for example that companies may require the solution comprise a backend system where specific access control mechanisms will be developed to ensure that only registered parties have access to privacy sensitive information. Similarly on the item and tag level options such as "kill command", the integrated usage of alternate IDs, tag-level encryption, prevention of tag reuse, randomization of IDs may need to be elaborated. Corporate communications (see below Consideration #8) also need to be used effectively in educating consumers and users regarding the risks of RFID.

2.5 Consideration #5: Tag & Product Integration/Design Variations

For companies considering RFID, there is a vast array of design permutations including numerous variations in a tag's "form factors" and physical characteristics such as size, shape and materials. The number of options available for companies can be confusing and include sizes from a few mm to 10's of centimetres, casings from naked tags to washable injection-moulded tags to glass or plastic covered tags, and shapes from square to circular to other multi dimensional designs. Tags can be integrated into, or merely applied onto, products or their packaging. With this amount of choice available on tag design - added to the frequency debate - companies are understandably concerned about selecting both the correct solution as well as the correct integration/attachment method. Moreover, the integration/attachment method is crucial from both a product integrity as well as aesthetic perspective. In the case of luxury goods for example, the RFID tag cannot interfere with the look and feel of the product and should ideally be covertly placed; similarly for the pharmaceutical or aviation industry the tag cannot interfere with the product integrity. These considerations have to be concluded prior to adopting the technology since if done incorrectly can jeopardize any rollout of the technology and its acceptance by companies.

Relevance to SToP:
Although RFID is usually an IT or logistics department driven initiative, it is essential companies consider and finalise product design and tag integration both early and substantially in the project. Having a technology that works is one thing, making it work in a product is entirely a different thing. Doing this only later in the process could result, at best, in having to reverse or undo the entire project and decisions and restart the planning and selection from the beginning; at worst it could result in belated cancellation of the initiative.

2.6 Consideration #6: Business Integration

Business integration, as opposed to product integration above, covers both system integration - the incorporation of RFID infrastructure (readers and tags) into production lines and processes; and IT integration – the linking of RFID systems and data transfer to enterprise systems. Integration is often the single biggest concern for managers [FER04]

From a system integration perspective, it is important to ascertain at what point in the supply chain tags will be added to products. There are three options to adding tags either:

- at product manufacture
- on the production line
- at the point of sale

The tradeoff between the three options is that cost decreases as one moves down the list above since less infrastructure adaptations and investment is required (eg production line machinery, production line speed, infrastructure changes etc), but at the same time the supply chain is less secure due to the audit trail being less extensive

due to the RFID system and associated data capture being introduced further along the supply chain.
From an IT integration perspective, the challenges of RFID implementation comes from integrating RFID systems and the data they generate with other functional databases and applications. Other implementation issues relate more to the effective use of the massive data captured by RFID systems and the incorporation of RFID technology throughout the whole supply chain - RFID systems implementation can generate large volumes as much as 30 times more data compared to pre RFID levels [WIDE04]

Proper deployment, by definition, means having the identification data being integrated into a wide variety of areas of the company. The challenge is not only with putting RFID tags on every item travelling around the world, but also with building the systems that make decisions based on item visibility events. Such events occur not only in the company's supply chain, but also in trading partners' supply chains, and all the ripple effects those events create.

Relevance to SToP:
End users in the SToP consortium need item level tagging to ensure the ability to identify and authenticate individual products. This effectively means that RFID tags and other authentication features can be added anywhere along the supply chain prior to retail levels. Companies will need to identify the point at which required data level and product pedigree information intersect with acceptable costs – obviously the earlier in the supply chain that RFID based anti-counterfeiting solutions are implemented, the more secure the supply chain and the more control can be exerted over products to reduce illicit trade. IT system integration is covered in more detail in other work packages - as identified in WP 3 and 4 deliverables, SToP will develop both the RFID hardware and software - Product Verification Systems (PVI) - to address these challenges.

2.7 Deployment of RFID Systems and Infrastructure

Companies need to accurately identify their requirements, select a technology, and then analyse, design and plan for production, assembling and integration into their products and processes. The right planning and strategy will give a company the best chance to achieve successful adoption and rollout, and a substantial return on investment. The implementer who blindly and superficially starts tagging will miss most of the benefits of this technology [KCSJ04]. The following discussion presents the key infrastructure and process areas that need to be realised prior to and during implementation. A methodical approach is required for the implementation and execution of RFID rollout including a detailed understanding of the processes and environments where the system will be installed and integrated, as well as an in depth analysis of requisite RFID infrastructure - readers and tags.

2.7.1 Reader Selection and Deployment

Readers can be deployed in a number of permutations comprising fixed, portable, or handheld readers, for each of UHF, HF, LF frequencies. To deploy the optimal system, substantial engineering time and effort needs to go into i) frequency and technology selection, followed by ii) the design of a read point including portable/fixed/handheld, antenna height/angle/size, protective covering or shielding, electromagnetic radiation compliance etc. The effort to precisely define, design, and implement large numbers of read points even for a single frequency can be significant.

In addition, due to an immature RFID supply chain, lead times for products can be long so it is important to ensure that the supplier has the necessary product available when it is needed. The RFID tag supply chain is still relatively immature with limited and inconsistent capacity to fulfil reader and tag orders; this will improve over time but for now this is an important consideration when deploying RFID.

2.7.2 Tags Selection and Deployment

Tags are the most important component of RFID implementation and tag purchases may be far more complicated than expected. Tags must provide the requisite performance, be easily integratable, and be capable of withstanding the full production and distribution challenges and environments including shipping wear, temperature extremes, and material handling machinery. In the simplest case – read-only tags – the tag has a pre-programmed unique number that cannot be changed. Read-write tags on the other hand can be updated and changed ie they contain a dynamic data memory that can be both written to and read from Memory size ranges from 2 kilobits, which is typical for inductive systems, up to 256 kilobytes for systems in the UHF and microwave ranges. Some of these read-write systems come with cryptographic functions for reciprocal authentication and for encryption of data traffic. Important considerations, in no special order, when selecting a tag for supply chain use include [KCSJ04]
:

- sensitivity: the ability of a chip to receive and send a signal of sufficient strength from and to a reader
- orientation: the effect of orientation of the tag in the read volume
- tag proximity: tags can interfere with each other when stacked close together.
- form factor: larger tags have longer ranges, but size & format is limited by product specs
- read speed: the amount of time required for a tag/s to be read (stationary or on conveyor)
- memory requirements: tags will require different memory and size depending on use
- RF interference: read rates are affected by RF noise, proximity to other tags, metal, and organic materials
- global regulations: tags may have different performances due to different authorized frequencies and global standards
- collision avoidance: the number of tags that must be read simultaneously in a given area
- security: not all security measures and encryption are supported by all tags
- memory: while many RFID tags have read/write capability (the ID / data on the tag can be changed ‘electronically’), from a practical perspective there are

few processes that should ever change the RFID tag data – instead tags should be used as 'license plates' that point to central databases that store the complete tag history and data.

Tags can be incorporated into a number of different forms including labels (affixed to products), laminated cards or cardboard tickets (carried by a person), plastic injection moulded tags (for harsh environments and metal mounting), and integratable tags (using various techniques to integrate directly into the products).

Thus questions then to answer prior to deployment include

- what size finished tag is necessary, and will it be overtly or covertly placed
- what is the maximum read range from the products being read, will multiple tags need to be read simultaneously and if so, how many
- are products on conveyor belts: what is the minimum time available to read
- how will the tag be applied; manually or automated applicator, or integrated, and must the tag be permanent or removable
- what are the typical environmental conditions in which the tag must operate, including minimum & maximum temperatures and humidity, water, chemicals, solvents, metals, or mechanical impacts
- does the tag need to be read only or read-write
- does anything need to be printed on the tag
- what is the anticipated tag life required,
- what volume of tags are required and over what period of time, what is the target price for the tags

Relevance to SToP:
Most users have limited insight as to how much engineering goes into the design and manufacture of RFID system components (reader, tag or labels) - there are so many variables that affect price and, more importantly, performance. Readers and tags are not created equally, require planning to purchase, and can have a delivery lead time of up to 18 weeks. Thus different reader/tag/label/inlay sources need to be identified and characterized according to various practical parameters.

To finalise tag selection, tests need to be conducted on density, speed, distance and resilience. These tests should be performed prior to product integration, as well as in situ following tag integration into the respective products. Important density measurements include identification of all tags, how many reads are acquired per second, and how long tag/s must remain in the read field to be read. Testing speed and distance is important to mimick real-world demands and providing an indication of how receptive the tag is and how efficient it is at functioning in the RF environment (important measurements include testing each tag in different orientations at different distances from the RF source signal, and at different speeds eg stationary, on a conveyor belt etc). Resilience testing analyses a typical tag life under conditions and processes similar to the real world application into which they will be deployed.

Finally testing for environmental influence includes subjecting the tag to direct sunlight, pressure, vibration, dropping tags from a height, immersion in water etc.

All tag tests should be conducted with individual 'naked' tags, single labels, multiple labels, and tags both integrated and/or affixed to products either covertly or overtly.Any problems identified during testing must be quantified, understood, and resolved including tag and reader compatibility, read range and speed of movement of the label through the read area, tag to reader orientation, EMI emissions in the environment, interference from case contents, damage during label application, placement of label on packaging consistent with case analysis [KCSJ04]

3 Pilot Analysis and Preparation

Companies in the SToP project have familiarized and educated themselves about RFID and have identified a pain-point where they think that RFID technology can best be utilized and deployed ie to reduce counterfeiting. After picking that point, extensive analysis has been carried out to select and test the most appropriate technology (as outlined in this document), following which the in line trial phase will be implemented and the data analysed. This process will quickly establish a good technology fit (or otherwise) and the potential for ROI. The pilot can then be extended more broadly in the company, with the outputs analyzed each step to confirm/determine the ROI at the various levels. This approach is employed in SToP in WP4 and WP5; the same process can be applied to any company in any industry independently considering the adoption of RFID for anti-counterfeiting purposes. Once it is determined that a full enterprise rollout would be effective and rewarding, it can be executed.

The above considerations have been applied to the SToP focus industries – Aviation, Luxury Goods, and Pharmaceutical; and companies – Airbus, Richemont, and The pharmaceutical industry. This process is discussed below in detail. Information has been obtained, analysed and researched from a broad arrangement of sources including semi structured interviews, project partner's experience and research, web research and publications.

3.1 Aviation:

3.1.1 Business Requirements:

For Airbus the main drivers for selection of a technology are as follows:

Criteria	Specifications
Consideration #1: Performance Criteria	Passive RFID with a long lifespan capable of operating in robust conditions without interfering with aircraft systems
Consideration #2: Cost	Depends on the item being tagged but given price of parts being tagged tag, costs are less important
Consideration #3: Standards	Important alignment and/or conformity with aviation industry Spec 2000 aerospace industry standards essential (more important than EPC/GS1 standards)
Consideration #4: Security and privacy risks	Use of cryptographic tags preferred High degree of confidence greater than Sigma 3 Tamper proof and resistant, should break upon detachment
Consideration #5: Tag Integration/Design	Affixed or adhesive, strong integration required to avoid tag falling off, destructible if removed Diverse tag application materials Extreme environmental temperatures and pressures
Consideration #6: Business Integration	Introduced on production line Includes with partner companies, end users, and after sales service points
Consideration #7: Reader Selection	Ability to read and authenticate metal aviation parts in random orientation over a read range from a few centimetres up to 2m while stationary/moving slowly.
Consideration #8: Tags Selection	Read write functionality is required Very past read speed and writing rate; no interruption/time delays to be introduced into current processes Read rate 100% Life time 15 years
Other Considerations:	Online and offline functionality

Table 2 : Aviation Criteria

The focus of the aviation industry currently is the problem of suspected unapproved parts (SUP - defined as aviation part, device, or material that is used in the production process of an aircraft) which does not meet the requirements of an approved aviation part, and is thus a major threat to passenger safety. The threat of unsafe parts can be reduced through the implementation of a variety of technologies - such as packaging and labels, bar coding and in-product marking - but when compared to others RFID offers unique efficiencies due to its cost-effectiveness (especially as the implementation costs of the technology continue to decline), adaptability and scalability.

3.1.2 Analysis:

3.1.2.1 Role of Standards

Aviation requirements of an RFID system are both stringent and demanding. As a framework for consideration, more precise specifications have been provided by the FAA and EASA who have agreed that passive RFID devices comply with applicable regulations and do not impact form, fit, or function of installed systems and equipment. The aerospace standard AS 5678 proposes the following feature for RFID device use in aircraft

- passive, reader talk first protocol
- 860 - 960 MHz frequency range
- read/write secure memory
- complies with ATA SPEC 2000 Chapter 9 *[ATA00]*
- environmental tests per DO 160E requirements
- metal mount, surface insensitive packaging
- 20 year service life
- complies with FAA policy dated May 13, 2005 [FAA05]
- air interface in accordance with EPCglobal (ISO 18000-6C) [EPC04]

3.1.2.2 Technology

Converting the standard requirements identified above into technology specifications for development will require the following semiconductor design parameters

- *memory*: the initial RFID chip will hold 64 kb of data of which 60 kb are user data; and 4 kb are reserved for EPC and memory management
- *header*: the header information (256 bits) will be completely EPC Class 1 Gen 2 compliant
- *maintenance*: an audit section for maintenance event records will be required (as per the Traceability Specification format defined in Spec 2000) *[ATA00]*. Each maintenance event will be no more than 170 characters long on the chip, and will start on an integer block boundary location to allow fast read access later.
- *data integrity:* maintenance events will not be written permanently onto the chip without first being logged and recorded (into the maintenance providers' record system). When the system of record has been updated then the IC block will be locked with a password so it cannot be overwritten or tampered with. If the record system cannot be updated simultaneously, then the block will not be permalocked, and the maintenance event data can still be written to the chip. When connectivity to the record system is established at a later time and the data logged there and confirmed that it is the same as the data on the chip, then that RFID data block can be locked on the chip.
- *data security:* once the data is permalocked on the chip (password-protected), the data cannot be over-written nor changed, thus creating a journal-type entry of maintenance events for that particular component. The most appropriate security features are still to be determined but currently it is important to ensure security between the different user zones (multi application card), and

that each zone can use a different set of passwords. A specific attempts counter for each password and for the authentication provides protection against systematic attacks. The full complement of security includes data security features (PKI): segregation between manufacturer, first user, second user, follow on users, controller capability on tag, and data management on tag.

Despite the UHF focus of the spec, both HF and UHF will be considered for the SToP project since both technologies can achieve essential performance parameters including tags that are able to tolerate the extreme hot and sub zero temperatures of ground operation and flying at altitude respectively; no risk of interfering with aircraft systems; capable of long read ranges and product orientations despite the heavy presence of metal in the products; read write functionality, and large memory capacity to provide full history and audit trail of the items. Low frequency, although also capable of achieving requisite performance criteria, is not considered due to apparent potential interference with aircraft systems.

For HF and UHF, various transponder types have been assessed and the following comparison on key aspects generated:

	HF 13,56MHz	**UHF 868 / 950 MHz**		
Antenna feature	Coil	Dipole		
Coupling	Induction RF	Radiation RF		
Read / Write distance	Close	Extendable		
Data density access	High	Low		
Multi object reading	Low anti collision probability	Anti collision capability		
Environmental influence	Useable on metal, fluids	Critical use on metal, in fluids and under coating		
Cost	Affordable	Low		
	HF 64kb	**UHF 64kb**	**UHF 2kb**	**EPC Gen 2**
Auto ID	X	X	X	X
Event Marking	Limited	X	X	X
C.M.	X	X		
Data Security	X			
Parts security	X			
ATA Comp.	X	X	X	Limited

Table 3 : HF and UHF Comparison

Once the IC requirements have been finalized, the chip is incorporated into an inlay comprising chip and tag to provide the final transponder for integration into the products. The antenna is designed according to the selected frequency (dipole for UHF versus coil for HF), read range (the greater the read range required the greater the ? required), and integration into products which determine form factor and protection.

3.1.3 Recommendations:

The goal of the industry is to have an electronic pedigree for each line replaceable unit (LRU - ie aviation parts that have to be replaced during the lifecycle of an aircraft) that documents its origin and its lifecycle, thus addressing the SUP threat to aircraft safety.

Selection of the transponder is the most crucial aspect for finalizing the technology to be utilized. Existing HF RFID devices appear most suitable due to high R/W memory capability up to 64kb and designed with security features (password, lock bit, crypto) to increase data security and part security. UHF device are likely not an option since UHF tags with with R/W memory capability will only be available in the near future, their performance is uncertain, and they cannot store all the maintenance information. Research is under way to increase the memory capability for UHF devices to address the AS5678 specification (eg Fujitsu 64kB FRAM).

For these reasons, the technology preference for the SToP project is HF initially, followed by UHF. The security capacity, memory size, and read/write speed of these options were essential to the choice of technology, and will be evaluated in the pilot.

The tag memory layout required for the above functionality is described in Appendix III; showing the memory arrangement of the data and how the data will be organized.

3.1.4 Essential Objectives:

The essential issues for the aviation industry to be evaluated and ensured in the pilot and subsequent deployment include:

- updatable RFID tag based data storage capacity of LRU UID and historical data is mandatory; including the reliability of tag writing, and tag reading (during interaction with a mobile device)
- historical data written to tags and correctly signed, including in an ambient working environment
- easy usability of the system
- failsafe operation of the synchronisation procedure between tags and the central database.

Deliverable 5.1 outlines the detailed program for the aviation industry design and deployment pilot project.

3.2 Luxury Goods:

3.2.1 Business Requirements:

For Richemont the main drivers for selection of a technology are as follows:

Criteria	Specifications
Consideration #1: Performance Criteria	Passive RFID capable of deep covert integration within metal and leather products.
Consideration #2: Cost	Low but not project decision critical; tagged products are typically very expensive relative to tags themselves
Consideration #3: Standards	Not necessary for closed loop anti-counterfeiting applications Need to function deep within metal - not possible with standard technology
Consideration #4: Security and privacy risks	High security required Cryptography requirements to be confirmed, in line with performance requirements such as bulk reading
Consideration #5: Tag Integration/Design	To be covertly placed within metal products (watches and jewellery) or leather products, without compromising aesthetic design of goods Performance essential to be maintained in RFID hostile environments such as metal Integrated covertly rather than affised
Consideration #6: Business Integration	Throughout supply chain starting with point of manufacture; including internally, partners, POS, customs, sales and after sales team
Consideration #7: Reader Selection	Ability to read and authenticate metal and leather luxury goods with read range from few cm up to 50cm in structured arrangement Read only functionality is sufficient.
Consideration #8: Tags Selection	Read only functionality sufficient initially Tag lifetime should cover lifetime of product – could be greater than 20 years for watches
Other Considerations:	Online and offline functionality required

Table 4 : Luxury Goods Criteria

Counterfeiting and diversion of luxury goods products will continue to be a problem due to the increasing sophistication of technologies for duplicating products and packaging, numerous wholesalers in the supply chain, weak legal penalties and lack of enforcement, and abundance of internet sites selling illicit products.

Technologies and processes that address these issues will be critical to the success of companies in this industry worldwide.

3.2.2 Analysis:

3.2.2.1 Current Standards Assessment

RFID standard technologies may be applicable for some of the luxury products such as leather goods, whereas for other products such as watches and jewellery where tags are placed/integrated within the metal non standard solutions are required due to their ability to deal with both the metal and large tag populations.

3.2.2.2 Watch Use Case:

This use case focuses on the covert integration of an RFID tag into a watch such that the RFID tag can be read through the metal casing. Different metals with different electromagnetic properties are used to manufacture watches and jewellery, and the influence of this varying metal composition on radiofrequency must be evaluated to design an appropriate and reliable RFID system.

i) Simulation at Low Frequency

The simulation of the magnetic field transmitted through a metal plate was made using a Quickfield 2D simulator calculation where a circular loop antenna is represented by two large metallic points - positive current in, and negative (same amplitude) current out; the frequency of the current variation used was 119600Hz.

Transit magnetic simulation requires precise definition of the loop antenna environment. The circular metallic watch casing is mimicked by a corresponding line with identical thickness. To accurately reflect the application being simulated, the simulated ‘tag’ is placed inside a closed metallic box. The following picture provides an example of the simulation. The magnetic field amplitude corresponds to the colour. Field is high for red (3000µT) and very low for purple (0 µT).

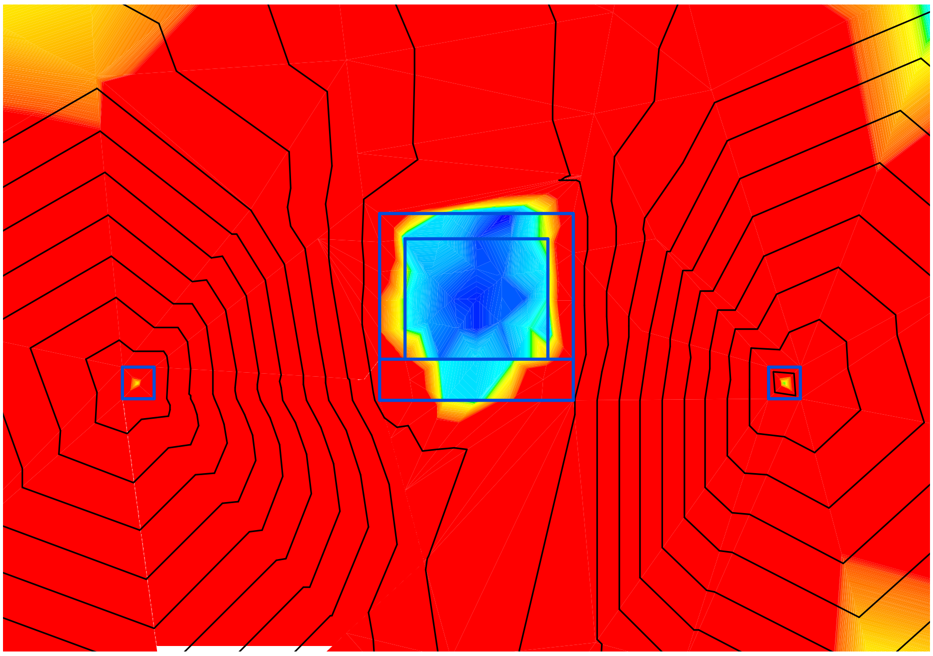

Figure 1 : Metal Case Electromagnetic Simulation @125kHz

The antenna corresponds to the two small blue squares on either side of the metal box which is in the middle of the diagram

Two parameters are used to define the metal material used: permittivity µ and conductivity in siemens per meter. Maxwells equation is closely mimicked using various input parameters (Mech) to define it.

The following curves provide simulation results for various metals that may be used in watches and jewellery including:

- poor conductor material: palladium and platinum showing similar behavior
- good conductor material : gold, copper, silver
- ferromagnetic material represented by one kind of steel (with µ equal to a thousand)

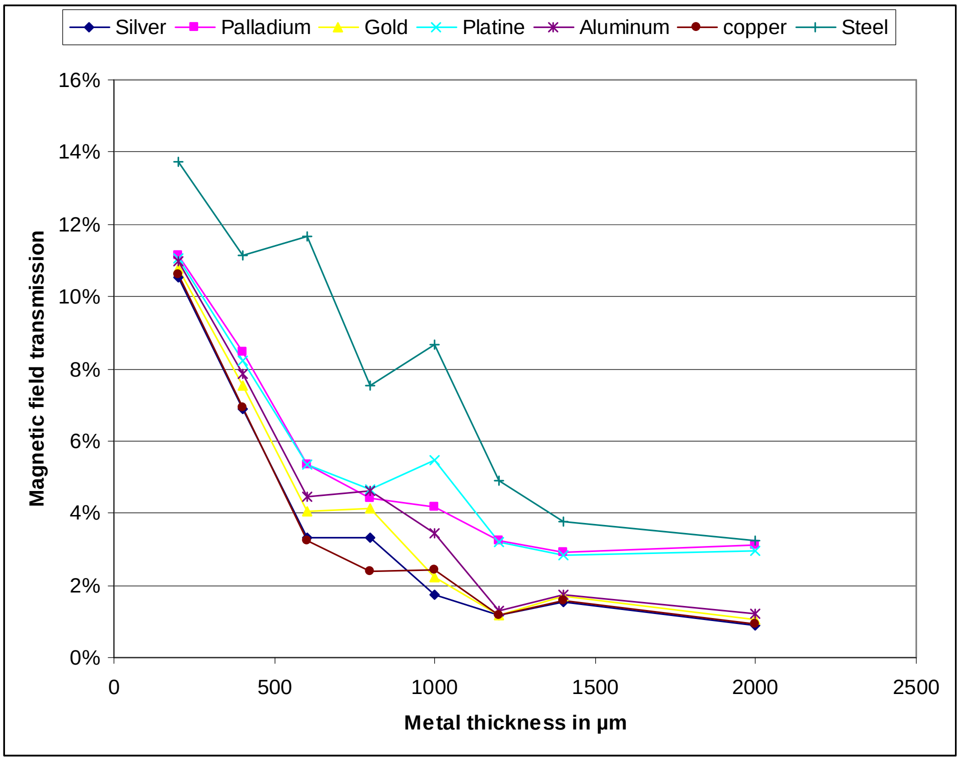

Figure 2 : RF Field Impact vs Metal Thickness

The simulation shows that, using low frequency, the effect of metal can be addressed; different metals result in different magnetic field strength and penetration. In real life, an average of the results is a good working hypotheses to work with prior to real life testing and implementation.

Electrical conductivity @ 20°C

- palladium : 9,5e6 s/m
- platinum : 9,6e6 s/m
- iron : 9,93e6 s/m
- zinc : 16,6e6 s/m
- aluminium : 37.8e6 s/m
- gold : 45,2e6 s/m
- copper : 59,6e6 s/m
- silver : 63e6 s/m

Steel is an alloy consisting mostly of iron, with a carbon content between 0.02% and 1.7 or 2.04% by weight. Brass is any alloy of copper and zinc; the proportions of zinc and copper can be varied to create a range of brasses, each of which has unique properties.

ii) Impact On Real Tag

A loop antenna of 8mm diameter and 300µm thickness corresponds to a tag sensitivity of around 100µT.

Inputting this to the simulation above; if for instance the metal plate thickness is 1mm, and knowing also that for a 4cm reader antenna diameter the magnetic field is approximately 2000µT, the ratio cannot be higher than 5%. According to Figure 2, this indicates that the tag can work with steel and platinum.

iii) Reading Distance

When metal is dominant, and when the tag needs to be read through metal, the reading distance is always reduced to a very short range. The following curve illustrates how the magnetic field created by a 4cm diameter loop decreases versus distance up to 10 centimetres. The magnetic field thus follows the law : $B(d) = \frac{\mu_0 * I * r_1^2}{2 * \sqrt{r_1^2 + d_1^2}}$

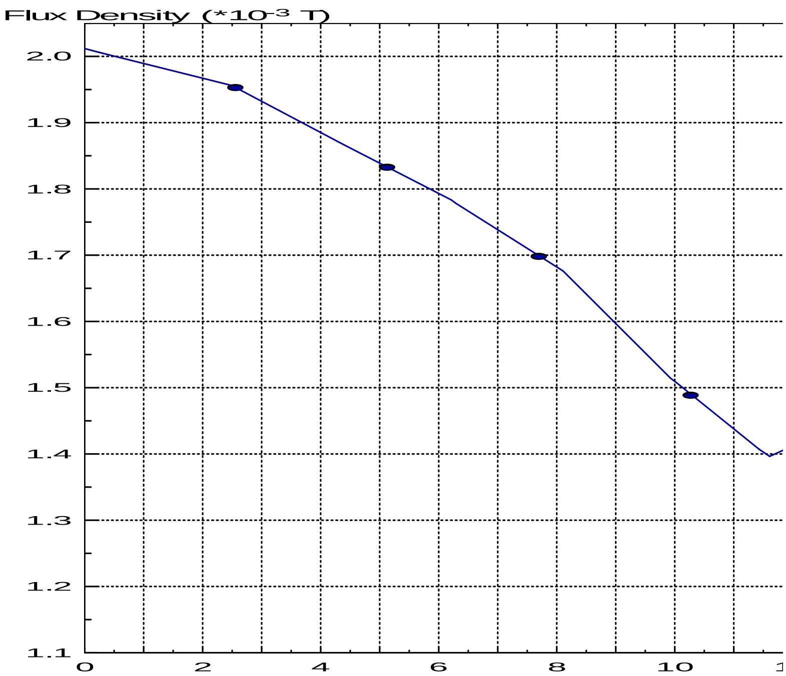

Figure 3 : Flux Density vs Distance

Reading distance thus depends on:
- surface of metal in front of the reader antenna
- thickness of metal plate
- metal type (mainly electrical conductivity)

Assuming that maximum magnetic field on the antenna is 2mT and assuming that tag sensitivity is 100µT, the read range can be estimated versus thickness of the metal plate and material type.

The following table gives the minimum magnetic field required to supply tags in front of a metal plate:

	200	**400**	**500**	**600**	**800**	**1000**	**1200**	**1400**	**2000**
Silver	950	1452	*2102*	*3013*	*4015*	*5809*	*8422*	*6541*	*11367*
Palladium	899	1183	1300	1874	*2261*	*2392*	*3085*	*3408*	*3226*
Gold	927	1327	1964	*2481*	*2431*	*4518*	*8422*	*5902*	*9548*
Platinum	904	1214	1658	1874	*2153*	*1832*	*3116*	*3507*	*3362*
Aluminum	910	1273	1690	*2249*	*2174*	*2904*	*7600*	*5762*	*8231*
Copper	944	1440	*2050*	*3067*	*4187*	*4149*	*8422*	*6368*	*10850*
Steel	729	898	912	856	1330	1155	*2037*	*2659*	*3100*

Table 5 : Metal Thickness Impact On RF Field

It is not possible to generate sufficient magnetic field where the value required is greater than 2mT (see values in italics).

Using the curve above, the read range for any kind of metal with thickness below 500µm will be greater than 10cm. For steel, the read range should be better than 10cm for thicknesses up to 1000 or 1200 µm. This does however also depend on reader antenna shape.

iv) Metal Impact For High Frequency

The same approach is used to illustrate the effect of metal on High Frequency. These simulations are done at 13,56MHz. Assuming a tag sensitivity of around 1µT, simulations were performed using the same mechanical environment to evaluate the HF system performances through metal.

Starting with a metal layer of 500µm, the magnetic field measured just behind the metal is around nano Tesla. This means that no HF solution exists to read across a metal plate with thickness greater than around 500µm.

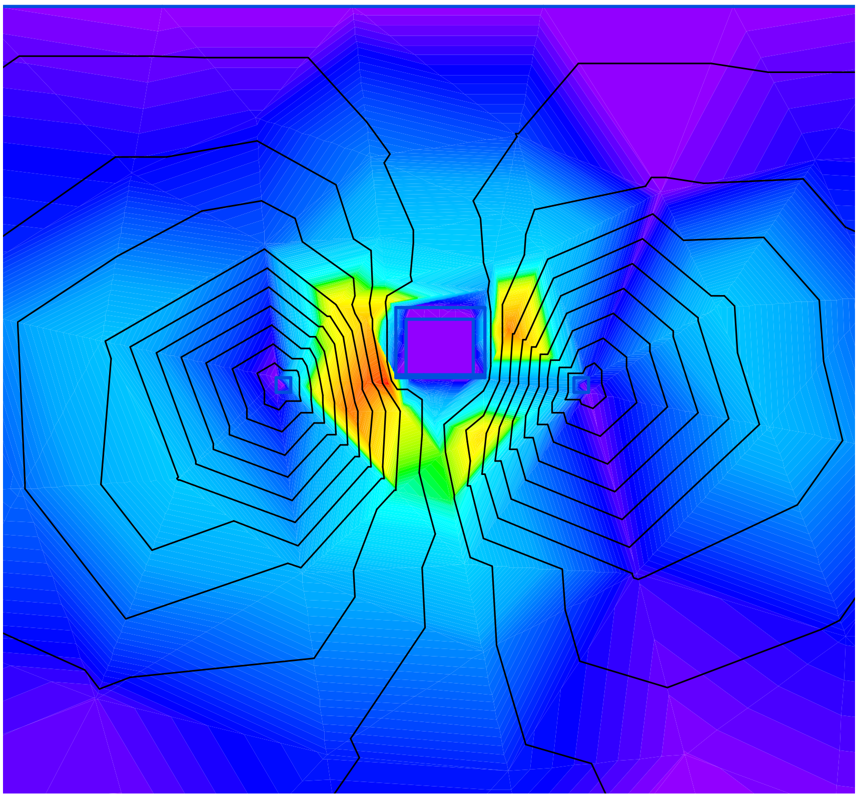

Figure 4 : Metal Case Electromagnetic Simulation @13,56MhZ

The magnetic field inside the box is lower than .3µT, thus there is no solution using this frequency. It may be possible to identify through metals of thickness less than 100µm, but this does not support any feasible real life implementation. This hypotheses was confirmed in real life testing of various solutions

v) Metal Impact on UHF Tags 900MHz

Simulation similarly shows no way to work through metal using UHF. Experimentations were also conducted using various kinds of readers and numerous different types of tags, without success.

vi) Simulation at High Frequency and Ultra High Frequency

Given the physics of the various frequencies; the simulation conducted served to confirm the fact that the heavy metal content of the watches incapacitates technologies operating at these frequencies, thus eliminating them as candidate solutions.

3.2.2.3 Leather Good Use Case

For this use case, several approaches were tested. A preliminary evaluation of the RFID constraints and security features gives us a list of RFID technology useable with leather goods.

Approach / Tag	UHF	HF		LF
Protocol	EPC Gen 2	ISO 15693	ISO 14443	ISO 18002
ID validity check	X	X	X	X
Track and trace	X	X	individually	individually
Password-based authentication	X	X	X	
Authentication with synchronized secret (RW-capabilities)		X	X	
Cryptographic authentication			X	

Table 6 : Frequency Comparison

i) EPC Gen2 Protocol

The EPC gen2 protocol was evaluated for track and trace capability since this protocol allows fast bulk identification with a data transfer up to 640kb/s. Small UFH tags using near field communication exist on the market and have a reading distance up to 50cm.

The advantages of this from a SToP and anti-counterfeiting perspective are the small tag dimensions, suppleness of the tag, bulk reading capability and track and trace functionality. The disadvantages however include limited write data capability, memory size, tag security features, readability in presence of metallic parts, and international regulations.

ii) ISO 15693 Protocol

The ISO 15693 protocol is the basis for contactless smartcards designed for use over distances of up to one metre. This range makes them a good fit for bulk reading applications; however for the integration into small leather goods eg wallets, the tag size must be as small as possible which will make bulk identification more difficult to perform.. This protocol allows a data transfer up to 26,6kb/sec and some products with read /write capability and security features (multi password protection, encryption) are available.

Advantage of this option include suppleness/flexibility of the tag, read and write capability, security features with password, and the availability of hand held readers (PDA cards). Disadvantages include readability in the presence of metallic parts, and tag size vs reading distance.

iii) ISO 14443 Protocol

The protocol ISO 14443 is a four-part international standard for contactless smart cards operating at 13.56 MHz in close proximity with a reader antenna. Contactless smart cards are intended to operate within up to 10cm of the reader antenna at a frequency of 13.56 MHz. The 13.56 MHz frequency was chosen for various technical reasons (e.g. suitability for efficient proximity inductive coupling, compliance with EMC regulation (already allocated as ISM band), low absorption by human tissues and more).
This protocol allows a data transfer up to 106kb/sec, products from manufacturers such as NXP (DESFIRE), Infineon and Texas Instruments have excellent characteristics such as large data memory (up to 4 Kbytes) and high security (3DES encryption).

The advantages of this protocol include very high data security (based on the use in electronic passport initiatives), suppleness of the tag, fast communication protocol, and hand held reader availability (NFC mobile phone). Disadvantages include low read range, and limited used and not efficiency for track and trace applications and bulk reading.

iv) Low Frequency
ISO 18000-2 is the standard defining parameters for Air Interface Communications below 135KHz, that is, the LF range.

Low frequency is the oldest adopted RFID technology, which has been implemented mostly in manufacturing and agricultural applications. ISO 11784 and 11785 are the two notable standards in the low frequency technology that has been in use for some time in animal tracking.

Advantages include the enhanced performance and ability to deal with metal; and the fact that the frequency is used worldwide without restrictions. Disadvantages include low data rate and the fact that most LF systems can only read one transponder at a time and do not support simultaneous reading of multiple items. A proprietary solution developed by SPACECODE does permit the reading of multiple items.

3.2.3 Recommendations

The objectives of the SToP trials are to demonstrate the feasibility of an effective and efficient authentication process for two different types of products – watches and leather goods. The main focus of the lab trials is to demonstrate the successful integration of tags into products (including in a metallic environment) where the integrated tags is readable irrespective of the metal, and able to successfully and easily validate authenticity of the product.

Watches and Jewellery: After thorough electromagnetic simulations and preliminary real life testing, the only way to read a RFID tag though metal is to use the lowest frequency authorized for auto identification.

Leather Goods: After testing the three main RFID protocols will be tested to verify if the piece of metal present in the leather bag has an influence on the data read rate, if the bulk reading is reliable due to the possible close proximity of the tag.

3.2.4 Essential Objectives:

For metallic products the crucial issues to address focus on a solution that is fully reliable in this RFID hostile environment ie:

- tag integration in a small available space, surrounded by metal
- high level of security, probably including multiple combined security features (and natural features)

authentication of one object at a time, in random orientation, close proximity, rapidly
For leather goods the essential parameters include:

- pliable and easily integratable tag
- single and multi items identification and authentication, in random orientation
- high level of security

Deliverable 5.1 outlines the detailed program for the aviation industry design and deployment trials.

3.3 Pharmaceutical:

3.3.1 Business Requirements:

For the pharmaceutical industry the main drivers for selection of a technology are as follows:

Criteria	Specifications
Consideration #1: Performance Criteria	Passive RFID capable of reading RFID tags affixed to primary packaging of products, moving at speed on a conveyor belt.
Consideration #2: Cost	Low costs target price of €0.03 cent tag
Consideration #3: Standards	EPC/GS1 Standards preferred for open loop supply chain and scalability
Consideration #4: Security and privacy risks	High security required Cryprographic requirements to be confirmed; tags must not be clonable Tamper resistance important
Consideration #5: Tag Integration/Design	To be overtly/covertly placed on primary packaging of bottles, ampoules, syrups, blister etc Covert preferred due to security and privacy reasons Numerous scenarios and materials to be taken into account regarding tag application

	Constraints include liquid, metal and limited space availability
Consideration #6: Business Integration	Throughout supply chain starting with production line, and including internally, partners, POS, customs, sales and after sales team
Consideration #7: Reader Selection	Ability to read and authenticate products by up to 2m for pallets and closer for item level, using fixed or handheld readers
Consideration #8: Tags Selection	EPC compliant tags with appropriate form factors for integration Read only and read write 96 bit serial number Very high reading and writing speed (tbc) 100% reading rate Tag lifetime 1 – 3 years
Other considerations:	Online and offline functionality required

Table 7 : Pharmaceutical Criteria

By identifying unique items using radio waves, RFID will improve upon the 25-year standard of product identification and tracking through bar codes. Because radio waves don’t require line-of-sight (for a bar code to work, a scanner must see the bar code, which means that the bar code must be oriented toward a scanner to be read), an entire pallet of product can be identified and tracked instantly, just by passing through a reader mounted on a warehouse door. The capacity of RFID tags to contain enough data for the identification of unique items, combined with the ability to layer encryption and additional features, increases operating efficiencies and decreases labour costs while simultaneously increasing security levels.

3.3.2 Analysis:

3.3.2.1 Current Standards Assessment

From a standards perspective, while the FDA is not endorsing any one particular counterfeiting technology, it has identified RFID as a potential key technology (with a preference for standard technology; except in instances where standards do not work eg metal foils) for track-and-trace throughout the supply chain. Standards have a number of components ie data structure, data format, communications protocol/frequency. The data standards are a given to ensure consistency and operability; whereas the communications protocol/frequency will be driven by performance as to whether a standard or non standard solution will be required (which could become a standard in the future).

3.3.2.2 Technology

Most commonly, counterfeited drugs are manufactured in various countries and then enter U.S. and European supply chains via poorly regulated and monitored wholesalers. Although the majority of drugs are distributed through a limited number of mainstream wholesalers, thousands of small wholesalers make up a booming secondary market. While these secondary wholesalers may create operating efficiencies, their size and number also make it easy to lose track of product shipments in the distribution chain, creating opportunities to introduce counterfeit drugs. In an effort to impede such operations, alternate approaches are being used such as requiring drug pedigrees or embracing standard of unit-of-use packaging.

The need for additional, more-thorough track-and-trace capabilities will become critical as manufacturing and the pharmaceutical supply chain grows even more complex. An increased number of products within various distribution channels, along with a greater need to control the environmental sensitivity of biologics, will undoubtedly become the norm, not the exception. Unfortunately, with today's security technologies, there is simply no way of validating or tracking a drug's complete path from raw material to consumer purchase.

The problem is perpetuated and compounded by increasingly sophisticated technologies for duplicating packaging and labels, numerous small wholesalers buying and selling drugs, increase in high-cost drugs and blockbuster products, weak legal penalties and lack of enforcement, abundance of internet pharmacies, and differential pricing on a global basis.

No other technology alone can match RFID in enabling two of the most important requirements for combating counterfeit drugs - instant authentication and robust track-and-trace. With RFID, each unit has a unique number (SKU, or electronic product code EPC) that allows authentication at any point in the supply chain, thus ensuring all supply chain participants have access to real-time recorded audit trail about a drug's history in the supply chain eg about a drug's current and historical locations, time spent at all locations, record of ownership, packaging configurations, environmental storage conditions, delivery dates and other pertinent information.

The pharmaceutical industry will as far as possible employ standard solutions due to the complexity and scope of the open loop supply chain where integration with supply chain partners is essential for scalability, cost reduction, integration, and compliance with e-pedigree audit trail requirements for all products. The type of RFID most suitable for the pharmaceutical industry depends on the product being labelled: for bottles it's likely to be HF or UHF (including Near Field UHF) or a hybrid path of HF-UHF eg HF for boxes and UHF for pallets. This is because HF works better in liquids and metals than UHF, whereas UHF reads faster, further and encodes tags faster. For blister foils however, current standard technologies do not work and the most suitable technology to deal with the metal would be a LF anti-collision system; although more costly HF and UHF solutions are also being researched for this purpose but with limited success.

Irrespective of the frequency used, RFID will be a cornerstone technology to increase the security of the pharmaceutical supply chain and improve patient safety. Utilising industry standards, as well as an additional layer of authentication for pharmaceutical drugs in the supply chain, an authenticated radio frequency identification (RFID) capability will be created at the item level.

The framework employed to achieve this authenticated RFID combines globally accepted and deployed ISO/IEC standards for RFID and Public-Key Infrastructure (PKI) technologies; using all of item-, case- and pallet-level RFID tags. This tagging structure approach will result in a hierarchy 'nomenclature', so that a particular item-level tag can be associated with its original case or pallet. This code hierarchy allows for the tracking of individual items such that if a product is sold somewhere, and its parent case/ pallet tag does not match the pharmacy a shipment was sent to, this can easily be determined as illicit trade.

In addition to RFID, evaluation and analysis will also be conducted on Datamatrix barcodes. This combined platform provides an enhanced identification and authentication solution.

Shipments of pharmaceutical products can use bottles or blister foils as primary packaging.

3.3.2.3 Bottles and Cartons Use Case:

Most pharmaceutical products in the US are shipped in bottles and cartons. Tests conducted using RFID for such bottles indicate that all of HF, UHF, and LF technologies can be used successfully to track, trace and authenticate these products. Given that EPC standards for such products are focussed on UHF and HF; the following preliminary and limited tests have been conducted on only one aspect of RFID implementation - data encoding of various tags; given the central importance of this aspect in the use of RFID. A similar testing protocol is to be carried out on other aspects during the course of the project.

i. UHF Tests

Tests conducted on non aluminium packaging were conducted to assess the number of coding errors with the respective technologies. Ten different experiments were conducted utilising 4 different line speeds and no repetition. Three different suppliers were evaluated. Overview of the data set is provided using normality tests; the resulting data points are represented below.

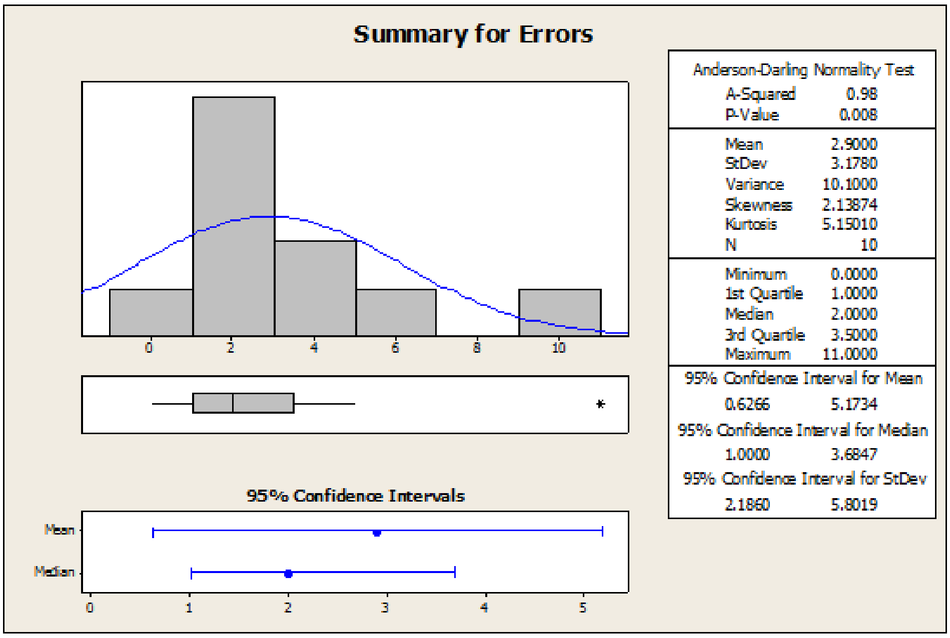

Figure 5 : UHF Encoding Summary Of Errors

Overall the data are normally distributed. The average number of defects is 2.9. The expected number of defects can vary from 0.6 up to 5.1. Further analysis of this defect rate focused on line speed and suppliers.

Line speed: Analysis concluded that the overall variation is not explained by the line speed which does not appear to be a significant factor (P > 0.05) - 14% only of the overall variation is explained by line speed.

Regression Analysis: Errors versus Line speed

The regression equation is

Errors = - 0.29 + 0.0225 Line speed

Predictor	Coef	SE Coef	T	P
Constant	-0.291	2.237	-0.13	0.900
Line speed	0.02247	0.01432	1.57	0.155

S = 2.94756 R-Sq = 23.5% R-Sq(adj) = 14.0%

Table 8 : Regression Analysis Errors vs Line Speed

The analysis of the residuals confirms the linearity of the model and the conclusion of the non influence of the line speed on the number of errors.

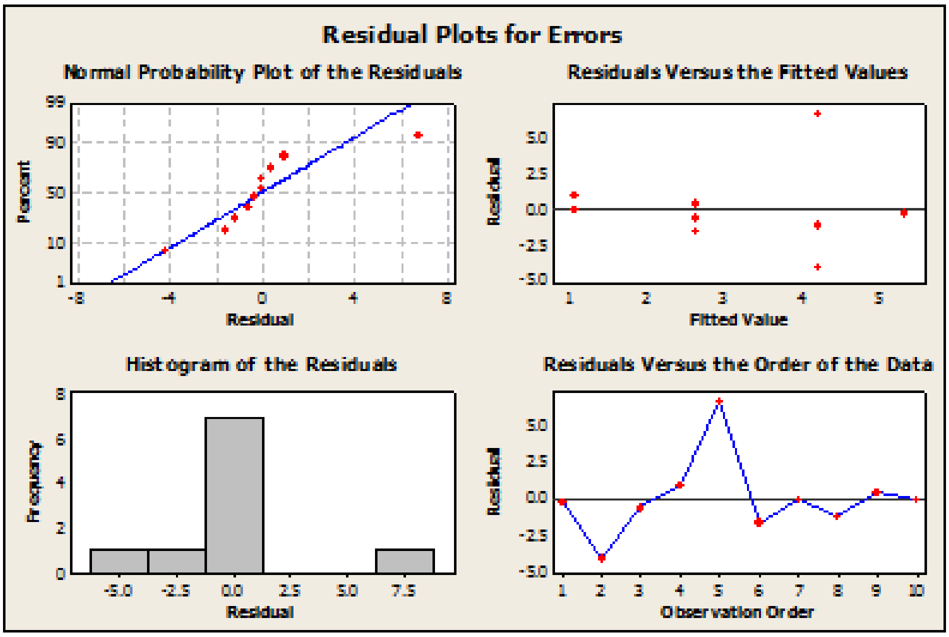

Figure 6 : UHF Encoding Residual Plots For Errors

There is a poor correlation between line speed and the number of errors.

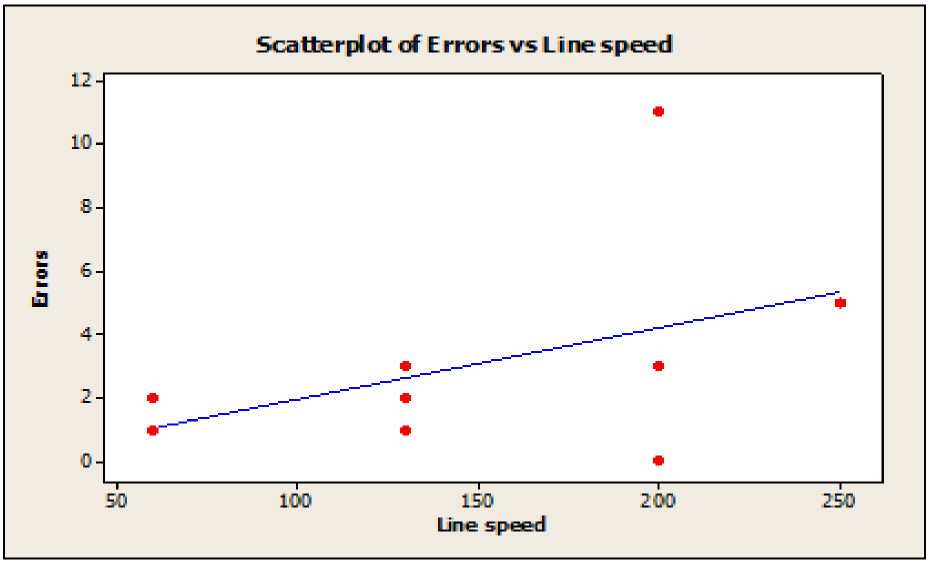

Figure 7 : UHF Encoding Scatterplot

Supplier: Similar analysis of the effect of suppliers demonstrated no influence. The c^2 test proved there is no difference among suppliers:

Chi-Square Test: Avery, Alien, Omron

```
Expected counts are printed below observed counts

Chi-Square contributions are printed below expected counts

          Avery    Alien    Omron  Total

    1      4224     2862     3102  10188

        4220.99  2866.84  3100.18

          0.002    0.008    0.001

    2         9       13        7     29

          12.01     8.16     8.82

          0.757    2.870    0.377

Total      4233     2875     3109  10217

Chi-Sq = 4.015, DF = 2, P-Value = 0.134
```

Table 9: UHF Regression Analysis Errors vs Line Speed

Translating this information into average proportion of defects observed and expected yields the following results where the overall proportion of defects is: 0.28%, and defect rates between 0 and 0.8% can be expected.

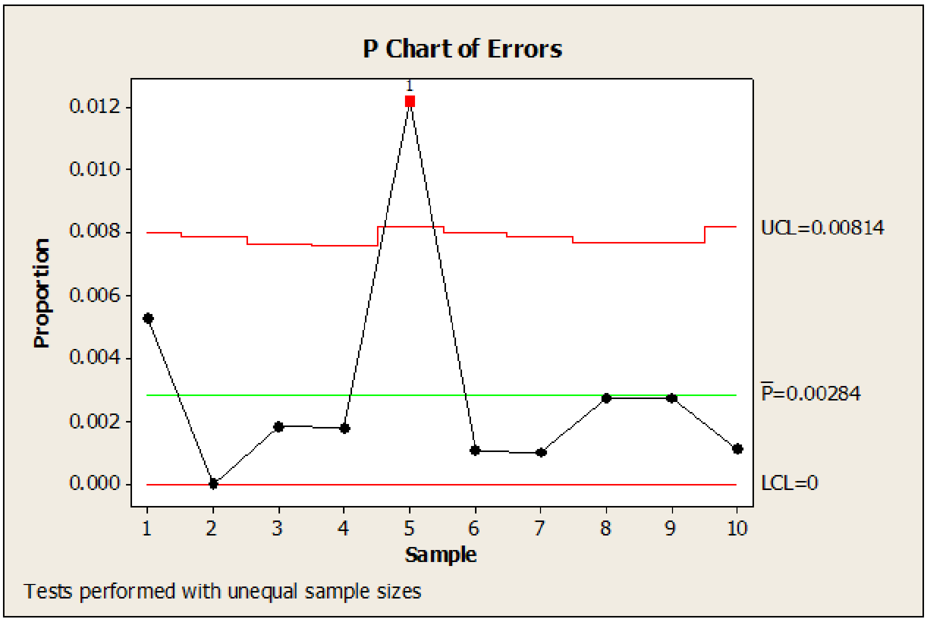

Figure 8: UHF Encoding Chart Of Errors

Conclusion: Based on these limited UHF tests, translation of defects rates into reject level means that the expected number of rejected tags per hour for a line running at 250 units/minute is 42 (based on rate of 0.28%). Using the typical size of a batch 36,000 units in the US, 100 tags would be rejected for encoding reasons only; this is excluding defects from labeling machine, readers, others. Further data and analysis is required from the pilots, looking at higher speeds and including repetitions of experiments to assess process stability and exploring other factors than line speed to control variation.

ii. HF Tests

A similar testing protocol was followed with HF.

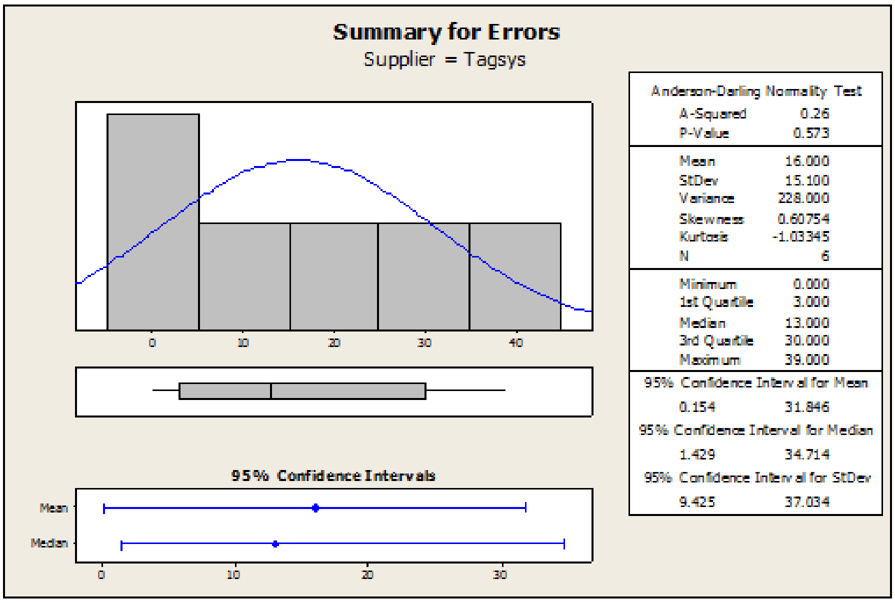

Figure 9: HF Encoding Summary Of Errors

Overall the data are not normally distributed. The median number of defects is 13. The expected number of defects can vary from 1.4 up to 34.7. The overall variation is not explained by the line speed (P > 0.05) - 39% only of the overall variation is explained by line speed.

Regression Analysis: Errors versus Line speed

The regression equation is

Errors = - 8.5 + 0.163 Line speed

Predictor	Coef	SE Coef	T	P
Constant	-8.50	12.94	-0.66	0.547
Line speed	0.16330	0.08004	2.04	0.111

S = 11.8178   R-Sq = 51.0%   R-Sq(adj) = 38.7%

Table 10: HF Regression Analysis Errors vs Line Speed

The analysis of the residuals confirms the linearity of the model and the conclusion of the non influence of the line speed on the number of errors.

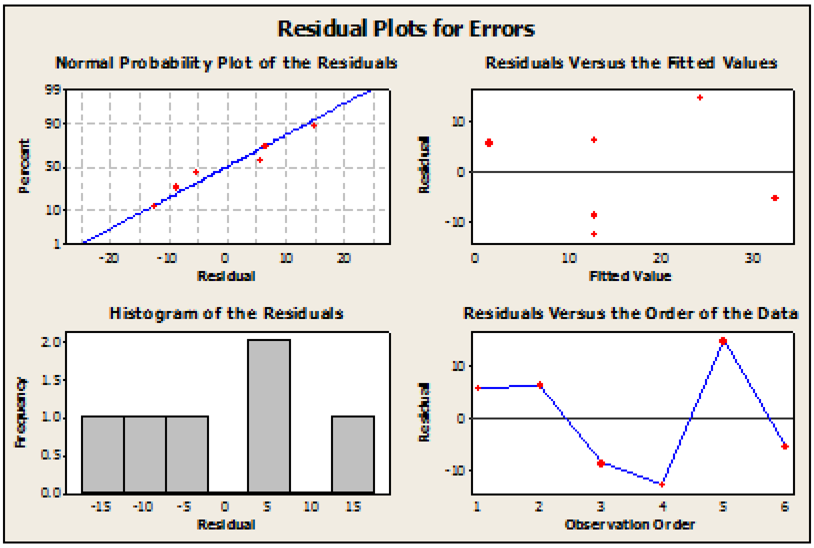

Figure 10: HF Encoding Residual Plot Of Errors

There is poor correlation between line speed and the number of errors.

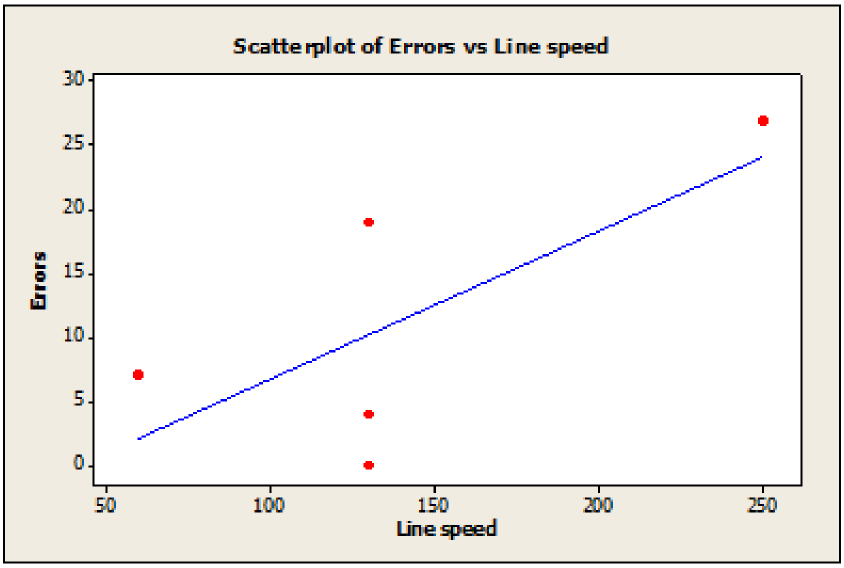

Figure 11: HF Scatterplot

The proportion of defects at high speed is: 2.6%; we could still expect defect rates between 1.1% and 4.2%

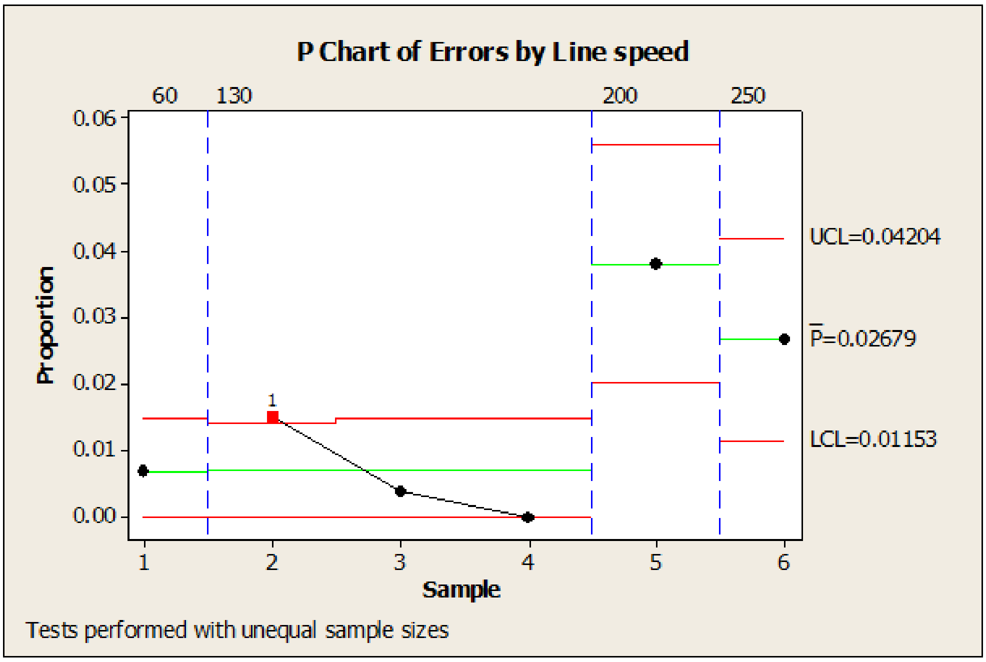

Figure 12: HF Chart of Errors

Conclusion: Translation of defects rates into reject level demonstrates that the expected number of rejected tags per hour for a line running at 250 units/minute is 405 (based on rate of 2.7%). The typical size of a batch being 36,000 units 972 tags would be rejected for encoding reasons only. All conclusions are valid only in the range of 60 to 250 units/minute: no extrapolation feasible.

3.3.2.4 Blisters Use Case:

When any metal is used as the primary packaging, standard EPC/ISO UHF and HF solutions experience reliability issues due to the effect of metal on the RF field. Tests conducted in this domain indicate that the pure physics dictate low frequency as the best choice due to its ability to deal with the metal in blister foils for drugs and medical devices (refer metal simulations in Luxury Goods sector).

RFID can incorporate dynamic tracking information into the supply chain to acquire a clear, accurate view of products as they travel from the manufacturing plant to the consumers' hands. By integrating RFID with security methods, all parties in the supply chain can access realtime, recorded authentication about a drug's entire history.

SPACECODE has developed a specific RFID label able to be read on an aluminium blister.

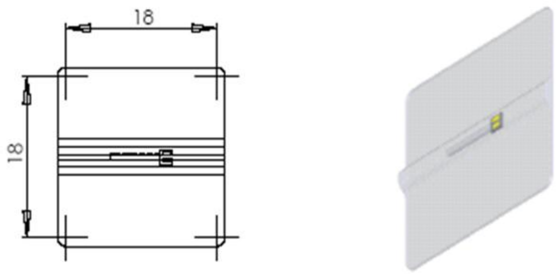

Figure 5 : RFID label for blister

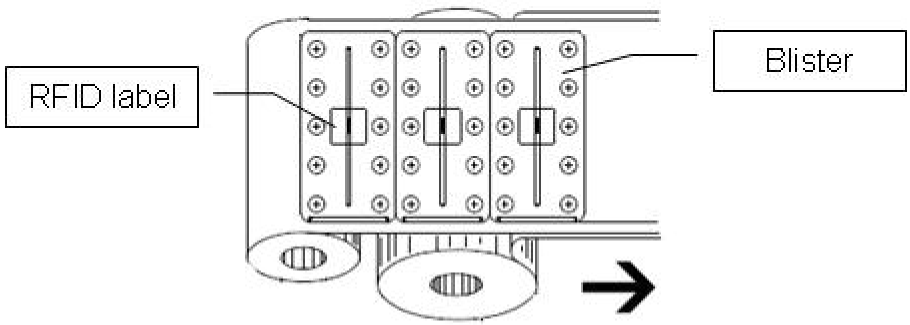

Figure 6 : RFID label on blister

The SPACECODE Aluminium Packaging solution is a RFID enabled metal/aluminium pack working with 100% accuracy despite being surrounded by and sealed within aluminium.

The 'SmartBlister' is used global commercial drug supply as well as global clinical trial supplies. The blister pack RFID technology allows full track and trace of blister packs with 100% accuracy and reliability.

3.3.3 Recommendations

The analysis determined whether UHF and HF tags can be applied, encoded and read at normal production speeds during packaging and distribution of pharmaceuticals. Verifying the authenticity of medications along each step of the distribution process adds an additional layer of security to reduce the chance of counterfeit pharmaceuticals entering the supply chain. It is also hoped that RFID data could improve efficiencies in the supply chain. The pilot will test the printing of data matrix codes on the line. Data Matrix offers high integrity data storage including data redundancy. This means that codes can be read even after sustaining some damage.

3.3.4 Essential Objectives:

For the pharmaceutical industry, essential issues to focus on include evaluation of a combined 2D barcode and RFID solution that operate sufficiently quickly without impacting or delaying the production line, in a secure and reliable fashion.

The key hardware success criteria include:

- complete reliability of data and technology
- hardware response time - RFID tags and 2D barcodes can be read within reasonable time.
- reliably detecting whether products are authentic or fake, or even diverted.
- correctly and fully determining the audit trail of a product
- accessibility, completeness, and relevance of information.
- usability

From a data encoding perspective, more detailed tests may be performed ie since both UHF and HF platforms show a high potential for defect reduction. In this regard important aspects to consider in evaluation of the pilot include the fact that more tests at higher speeds than 200 units/minute are needed, and more repetitions of experiments to be included to assess process stability at higher speeds than 130 Units/minute. Need to find other factor than line speed to control variation which in the analysis above excludes defects from labeling machine, readers, others. Aspects other than line speed will also be investigated to control: read range, encoding range, power etc.

The same tests will need to be conducted on 2D barcodes.

Deliverable 5.1 outlines the detailed program for the aviation industry design and deployment trials.

4 SToP Conclusion - A Continuous Chain of Assurance with RFID

When compared with other existing security technologies (for example, bar codes, in-product marking, tamper-evident packaging), RFID offers more robust and capable efficiencies. Manual involvement is decreased, because line-of-sight is not required for product scanning. Less product waste occurs, since verifying authenticity doesn't require product destruction. And unlike bar codes, RFID codes not only identify unique products, but are themselves unique and cannot be duplicated. They can also be encrypted for additional security. RFID tags carry substantially more information than bar codes, are scalable and reusable for much longer active-use lives and have faster read times for high throughput. While not a standalone solution, when implemented along with a layer of traditional security technologies and integrated with other enterprise applications, RFID can give a significantly more efficient means to accomplish product-safety and brand-protection goals.
Companies can leverage their existing infrastructures to simultaneously report on goods movement and status while feeding real-time tracking RFID data to multiple enterprise resource planning (ERP), supply-chain management and warehouse management systems (WMS). Unique IDs support creation of an international pedigree that can be verified at any point in the supply chain, creating a continuous chain that can be checked with confidence.

SToP end users recognise the benefits of this technology generally and have identified the anti-counterfeiting opportunity specifically. To ensure success, companies must strategically determine how current anti-counterfeiting initiatives and processes can be improved to become more secure, efficient, faster, and more accurate using RFID technology. And then they must actually be prepared to change their processes and plan accordingly with a view to reaping rewards.

The potential impact and strategic importance of the project is relevant in and applicable to the three areas or levels most affected by counterfeiting today: state, business and society. Reducing illicit trade using RFID (with or without other technologies) will have a massive impact towards solving key societal problems including socioeconomic effects (eg jobs are lost, investments are not made, and state revenue is diminished), risks to public health, and the overall well-being of consumers, and the profitability of large, medium, and smaller companies alike. The keys to success are threefold – correct selection of technology (WP3,4,5), adequate planning for deployment (WP4,5), and optimal utility of data through comprehensive data management (WP3) – all of which will result in achieving the objectives of SToP ie ubiquitous ambient intelligence infrastructure for anti-counterfeiting goals to massively reduce the scale and ease of counterfeiting. Irrespective of whether RFID alone or in combination is used, the same approach and preparation described above applies to any technology selected be it RFID, digital and/or optical techniques, LSA etc.

This paper has described what is required for successful RFID analysis, preparation, implementation and production to achieve smart and verifiable products in company supply chains that can eliminate the trade in illicit products. These findings and recommendations will be employed, tested, and improved following the real world live trials in WP5; followed by finalization and (re) documentation in Deliverable 4.4. The outputs and recommendations of these work packages focus on development of the corresponding ultimate real-world production and assembling processes that may be required, including impacts on affected machines and production lines to produce smart and verifiable products e.g. ‘smart’ watches, spare parts, and pharmaceuticals . New requirements imposed by the utilized smart tags will be identified and evaluated resulting in a cost-efficient solution that minimises any impact on the production line eg production time must not be prolonged. The proposed product verification processes will need to be accompanied by changes within the existing IT infrastructure related to supply chain processes including integration, data management, and deployment and connecting of novel RFID verification devices such as RFID readers and tags in the respective supply chain environments.

References

[ATA00] http://www.spec2000.com/50.html

[EPC04] Information technology -- Radio frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz

[FAA05] http://www.faa.gov/regulations_policies/policy_guidance/

[FER04] Ferguson, R.B., Taking on RFID Challenge, Eweek, 2004

[FIN06] Finkenzeller Klaus., RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 2006

[KCSJ04] Kleist R., Chapman T., Sakai D., Jarvis B., RFID Labeling: Smart Labeling Concepts & Applications for the Consumer Packaged Goods Supply Chain, 2004

[FLMA05] Fleisch, E., Mattern, F., Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis, 2005

[JUE05] Juels, A., RFID Security and Privacy: A Research Survey, IEEE Journal Selected Areas in Communications, 2005

[OCO05] O'Connor, M.C., "Alien Drops Tag Price to 12.9 Cents", RFID Journal (available at http://www.rfidjournal.com/article/articleview/1870/1/1/), 2005

[THI07] Thiesse, F., RFID, Privacy and the Perception of Risk: A Strategic Framework, 2007

[VIS06] Suhong, L. and Visich, J.K. Radio Frequency Identification: Supply Chain Impact and Implementation Challenges. International Journal of Integrated Supply Management, 2006

[WIDE04] Wilding, R., Delgado, T. RFID demystified: supply-chain applications, Logistics and Transport Focus, 2004

[WEI04] Weil, M., RFID confusion and possibility, APICS – the Performance Advantage, 2004

5 APPENDIX

5.1 Appendix I : RFID Overview

Similar to a barcode or smart card system, a radio frequency identification (RFID) system is an automatic identification system that can be used to uniquely label and identify objects or persons. A unique identifier is embedded into a microchip, which in turn is attached to a small antenna (chip plus antenna give a tag). The microchip can also incorporate functionality beyond simple identification and include integrated sensors, read/write storage, encryption and access control. The tag is then attached to an item, a case or a pallet. As the item/case/pallet moves into the scanning range of the reader, the reader sends out electromagnetic waves that form a magnetic field when they ‘couple’ with antenna on the RFID tag. The tag draws power from the magnetic field and uses it to power the microchips’ circuits. The microchip then modulates the received signal in accordance with its identification or programmed code and transmits or reflects a radio frequency signal whichis in turn picked up by the reader, which decodes the information contained in the transponder and either stores the information, acts upon it or transmits the information to the host computer via the communications port where the tag data are processed in a computer system, such as an inventory control system, an authentication system, or an access control system.

RFID systems are characterized by the fact that the reader and tag can communicate via
magnetic or electromagnetic fields without contact or line of sight. The tag draws all the energy it needs to communicate with the reader from the reader’s magnetic or electromagnetic field. Contactless information exchange sets RFID systems apart from other identification systems, such as barcodes and contact-dependent chip cards. In order to scan a barcode, line of sight is required. A chip card must directly touch a reader. The decisive performance parameters for RFID systems, including for anti-counterfeiting applications, are the range of the reader and the ability to penetrate liquids or metals with the field necessary for communication. These parameters are mainly determined by the coupling principle between the reader and tag and by the transmission frequency of the reader. A tag must be within a reader’s read range in order to be activated. Using special anti-collision communication protocols, it is also possible for a single reader to read multiple tags within its range in parallel (bulk reading or bulk processing).

5.2 Appendix II: Consortium End user Questionnaires

5.2.1 Aviation Questionnaire

1. General questions						
Who has ultimate responsibility in your organization for anti-counterfeiting initiatives and rollout?	IP ☐	Legal ☐	Logistics ☐	Business ☐	IT ☐	Other / Don't know: Quality Assurance
Should an anti-counterfeiting / product authentication system be linked to supply chain management systems?	Yes: ☒		No: ☐		Don't know: ☐	
Do you desire to use the anti-counterfeiting system to detect also diverted / parallel traded goods?	Yes: ☒		No: ☐		Don't know: ☐	
Please describe what experience, if any, you have with anti-counterfeiting technologies.	Document authentication processes, PKI on data exchange					
What are your main business objectives with anti-counterfeiting technology (i.e., what keeps you awake at night)?						

2. Which physical objects do you want to authenticate? (you can select one or more)	
Single products	☒ What kind of a product:
Cases	☐
Pallets	☐
Other, what?	

3. How important are these authentication modes?				
	High importance	Medium importance	Low or no importance	Don't know
Authentication of one object at a time	☒	☐	☐	☐

Authentication of multiple objects at once (e.g., bulk reading)	☐	☐	☒	☐

4. Where does the authentication take place? (evaluate the importance of different use cases)				
	High importance	Medium importance	Low importance	Don't know
In our own company (e.g., manufacturing plant, warehouse, distribution centre)	☒	☐	☐	☐
In a partner company (e.g., logistics forwarder, distributor, retailer)	☒	☐	☐	☐
In the point-of-sale (by a sales clerk)	☒	☐	☐	☐
In customs (by a customs officer)	☐	☐	☒	☐
By a private investigator	☐	☐	☒	☐
By consumer or end-user of the product	☒	☐	☐	☐
By after sales services (e.g., repair)	☒	☐	☐	☐
In other places, where?:	☐	☐	☐	☒

5. What are the features of the process and environment?		
What is the level of human oversight?	Authentication without human oversight, check has to be completely automated ☒	Check is done by a person who uses the authentication device ☐
If check is done on a conveyor, how fast does the conveyor move?		
How much metal is in the product or environment?		
How much organic/liquid is in the product or environment?		
Are the items to be read in close proximity to each other, to metal, etc.?		

Are the items to be read in random orientation?	Yes ☒	No ☐	Don't know ☐	
Are the readers to be handheld, portable, or fixed? (select all that is required)	Portable ☒	Handheld ☒	Fixed ☐	Don't know ☐
Does the system have to work in offline mode, without network connection?	Yes ☒	No ☐	Don't know ☐	

6. What are the requirements regarding performance?	
Read range required (max)	
No. of products to be checked per second	

7. What is the required output format of the authentication system? (select what is required)		
Output must clearly state authentic / not.	☒	
The output has to present suspicious/unclear cases for example by displaying the level of confidence (e.g., *medium confidence*, or 66%), when possible.	☒	
Output has to display also other information to facilitate a further physical / manual product check.	☒	If yes, what information?
Other, what?		

8. Other questions: (leave open if answer is unknown or question is not relevant)	
Where and by whom will the security labels be affixed? E.g., production line (beginning/end);	
What constraints are there for integration of the security feature? (e.g., material, space available)	

Is there a preferred integration method: adhesive, special covering, aesthetic covering, integrated invisibly into packaging	
What is the required life-time of the security feature?	
What environmental constraints are there for the security feature (e.g., temperature, pressure, robustness etc.)	
Can the security feature be visible, if also visible feature is secure enough?	
Are there any special requirements regarding tampering resistance?	

5.2.2 Luxury Goods Questionnaire

5.2.2.1 Watch use case

1. General questions						
Who has ultimate responsibility in your organization for anti-counterfeiting initiatives and rollout?	**IP** ☒	Legal ☐	Logistics ☐	Business ☐	IT	Other / Don't know: Quality Assurance
Should an anti-counterfeiting / product authentication system be linked to supply chain management systems?	**Yes:** ☒		No: ☐		Don't know: ☐	
Do you desire to use the anti-counterfeiting system to detect also diverted / parallel traded goods?	**Yes:** ☒		No: ☐		Don't know: ☐	
Please describe what experience, if any, you have with anti-counterfeiting technologies.	No specific technology (see D3.1, chapter 4.6) Main used technology to be considered is "Serialization" of the product via the visible individual number on the product					
What are your main business objectives with anti-counterfeiting technology (i.e., what keeps you awake at night)?	Allow a none-brand expert to identify a fake product - with less then 5 seconds - without using tools given aesthetic and technical specification, photo comparison					

2. Which physical objects do you want to authenticate? (you can select one or more)	
Single products	☒ What kind of a product: **Watches** Critical case to investigate: small model, square shape, backcase with crystal, quartz mechanisms, gold material.
Cases	☐ 2 main cases: - A: Product authentication by Staff having connection to internal information system - B: Product authentication by a external investigator
Pallets	☐
Other, what?	

3. How important are these authentication modes?				
	High importance	Medium importance	Low or no importance	Don't know
Authentication of one object at a time	☒	☐	☐	☐
Authentication of multiple objects at once (e.g., bulk reading)	☐	☒	☐	☐

4. Where does the authentication take place? (evaluate the importance of different use cases)				
	High importance	Medium importance	Low importance	Don't know
In our own company (e.g., manufacturing plant, warehouse, distribution centre)	☒	☐	☐	☐
In a partner company (e.g., logistics forwarder, distributor, retailer)	☒	☐	☐	☐
In the point-of-sale (by a sales clerk)	☒	☐	☐	☐
In customs (by a customs officer)	☒	☐	☐	☐
By a private investigator	☒	☐	☐	☐
By consumer or end-user of the product	☐	☐	☒	☐
By after sales services (e.g., repair)	☒	☐	☐	☐
In other places, where?:	☐	☐	☐	☐

5. What are the features of the process and environment?		
What is the level of human oversight?	Authentication without human oversight, check has to be completely automated ☐	**Check is done by a person who uses the authentication device X** ☐
If check is done on a conveyor, how fast does the conveyor move?	N/A	
How much metal is in the product or environment?	Everywhere (90% of metal + crystal + miscellaneous)	
How much organic/liquid is in the product or environment?	N/A	

Are the items to be read in close proximity to each other, to metal, etc.?	Yes, specially to metal Product distance is as well important (less than 10 cm)			
Are the items to be read in random orientation?	**Yes** **X (if possible)** ☒	No ☐	Don't know ☐	
Are the readers to be handheld, portable, or fixed? (select all that is required)	**Portable** **(Case B)** ☒	Handheld ☐	**Fixed** **(Case A)** ☒	Don't know ☐
Does the system have to work in offline mode, without network connection?	Yes ☐	**No** ☒	Don't know ☐	

6. What are the requirements regarding performance?	
Read range required (max)	No specification
No. of products to be checked per second	1 products very 5 seconds (max)

7. What is the required output format of the authentication system? (select what is required)		
Output must clearly state authentic / not.	☐	
The output has to present suspicious/unclear cases for example by displaying the level of confidence (e.g., *medium confidence*, or 66%), when possible.	☒	
Output has to display also other information to facilitate a further physical / manual product check.	☒	**If yes, what information? See User case #2 (RM)**
Other, what?	.	

8. Other questions: (leave open if answer is unknown or question is not relevant)	
Where and by whom will the security labels be affixed? E.g., production line (beginning/end);	Brand owner – Internal or external manufacture assembly line

What constraints are there for integration of the security feature? (e.g., material, space available)	No space in the product without material machining Size of the tag is key to minimize product modification
Is there a preferred integration method: adhesive, special covering, aesthetic covering, integrated invisibly into packaging	Integrated (visible and/or invisible) into the product
What is the required life-time of the security feature?	20 years
What environmental constraints are there for the security feature (e.g., temperature, pressure, robustness etc.)	Temperature: from -20C to +80C Pressure: 30 atm(bar) to 100atm Robustness: to be evaluated
Can the security feature be visible, if also visible feature is secure enough?	Only the individual number is visible Otherwise, cover (semi-cover) security feature is required due to aesthetic constraints
Are there any special requirements regarding tampering resistance?	The tampering must be identifiable

5.2.2.2 Leather good use case

1. General questions						
Who has ultimate responsibility in your organization for anti-counterfeiting initiatives and rollout?	**IP** ☒	Legal ☐	Logistics ☐	Business ☐	IT	Other / Don't know: Quality Assurance
Should an anti-counterfeiting / product authentication system be linked to supply chain management systems?	**Yes:** ☒		No: ☐		Don't know: ☐	
Do you desire to use the anti-counterfeiting system to detect also diverted / parallel traded goods?	**Yes:** ☒		No: ☐		Don't know: ☐	
Please describe what experience, if any, you have with anti-counterfeiting technologies.	No specific technology (see D3.1, chapter 4.6) Main used technology to be considered is "Serialization" of the product via the visible individual number on the product					
What are your main business objectives with anti-counterfeiting technology (i.e., what keeps you awake at night)?	Allow a none-brand expert to identify a fake product - with less then 1 second - without using tools given aesthetic and technical specification, photo comparison					

2. Which physical objects do you want to authenticate? (you can select one or more)	
Single products	☒ What kind of a product: **Leather goods** Critical case to investigate: small model (wallet),
Cases	☐ 2 main cases: - A: Product authentication by Staff having connection to internal information system - B: Product authentication by a external investigator
Pallets	☐
Other, what?	

3. How important are these authentication modes?

	High importance	Medium importance	Low or no importance	Don't know
Authentication of one object at a time	☐	☐	☒	☐
Authentication of multiple objects at once (e.g., bulk reading)	☒	☐	☐	☐

4. Where does the authentication take place? (evaluate the importance of different use cases)				
	High importance	Medium importance	Low importance	Don't know
In our own company (e.g., manufacturing plant, warehouse, distribution centre)	☒	☐	☐	☐
In a partner company (e.g., logistics forwarder, distributor, retailer)	☐	☒	☐	☐
In the point-of-sale (by a sales clerk)	☒	☐	☐	☐
In customs (by a customs officer)	☒	☐	☐	☐
By a private investigator	☒	☐	☐	☐
By consumer or end-user of the product	☐	☒	☐	☐
By after sales services (e.g., repair)	☒	☐	☐	☐
In other places, where?:	☐	☐	☐	☐

5. What are the features of the process and environment?		
What is the level of human oversight?	**Authentication without human oversight, check has to be completely automated X** ☐	Check is done by a person who uses the authentication device ☐
If check is done on a conveyor, how fast does the conveyor move?	200 products/items within maximum 5 seconds	
How much metal is in the product or environment?	Limited	
How much organic/liquid is in the product or environment?	N/A	

Are the items to be read in close proximity to each other, to metal, etc.?	Yes, Product distance to each other is less than 5 cm.			
Are the items to be read in random orientation?	**Yes** ☒	No ☐	Don't know ☐	
Are the readers to be handheld, portable, or fixed? (select all that is required)	**Portable (Case B)** ☒	Handheld ☐	**Fixed (Case A)** ☒	Don't know ☐
Does the system have to work in offline mode, without network connection?	Yes ☐	**No** ☒	Don't know ☐	

6. What are the requirements regarding performance?	
Read range required (max)	No specification
No. of products to be checked per second	200 products/items within maximum 5 seconds

7. What is the required output format of the authentication system? (select what is required)		
Output must clearly state authentic / not.	☒	
The output has to present suspicious/unclear cases for example by displaying the level of confidence (e.g., *medium confidence*, or 66%), when possible.	☐	
Output has to display also other information to facilitate a further physical / manual product check.	☐	
Other, what?	.	

8. Other questions: (leave open if answer is unknown or question is not relevant)	
Where and by whom will the security labels be affixed? E.g., production line (beginning/end);	Brand owner – Internal or external manufacture assembly line
What constraints are there for integration of the security feature? (e.g., material, space available)	Softness required (equivalent to the leather, fabric) Size of the tag is key to avoid aesthetic impact

Is there a preferred integration method: adhesive, special covering, aesthetic covering, integrated invisibly into packaging	Integrated (visible and/or invisible) into the product
What is the required life-time of the security feature?	10 years
What environmental constraints are there for the security feature (e.g., temperature, pressure, robustness etc.)	Temperature: from -20C to +80C, Pressing, Dry cleaner's etc…
Can the security feature be visible, if also visible feature is secure enough?	Only the individual number is visible Otherwise, cover (semi-cover) security feature is required due to aesthetic constraints
Are there any special requirements regarding tampering resistance?	The tampering must be identifiable

5.2.3 Pharmaceutical Industry Questionnaire

1. General questions						
Who has ultimate responsibility in your organization for anti-counterfeiting initiatives and rollout?	IP ☐	Legal ☐	Logistics ☐	Business ☐	IT ☐	Other / Don't know:
Should an anti-counterfeiting / product authentication system be linked to supply chain management systems?	Yes: ☒		No: ☐		Don't know: ☐	
Do you desire to use the anti-counterfeiting system to detect also diverted / parallel traded goods?	Yes: ☐		No: ☐		Don't know: ☒	
Please describe what experience, if any, you have with anti-counterfeiting technologies.						
What are your main business objectives with anti-counterfeiting technology (i.e., what keeps you awake at night)?						

2. Which physical objects do you want to authenticate? (you can select one or more)	
Single products	☒ What kind of a product:
Cases	☒
Pallets	☒
Other, what?	

3. How important are these authentication modes?				
	High	Medium	Low or no	Don't

	importance	importance	importance	know
Authentication of one object at a time	☒	☐	☐	☐
Authentication of multiple objects at once (e.g., bulk reading)	☐	☐	☒	☐

4. Where does the authentication take place? (evaluate the importance of different use cases)				
	High importance	Medium importance	Low importance	Don't know
In our own company (e.g., manufacturing plant, warehouse, distribution centre)	☒	☐	☐	☐
In a partner company (e.g., logistics forwarder, distributor, retailer)	☒	☐	☐	☐
In the point-of-sale (by a sales clerk)	☐	☒	☐	☐
In customs (by a customs officer)	☐	☒	☐	☐
By a private investigator	☐	☐	☐	☒
By consumer or end-user of the product	☐	☐	☒	☐
By after sales services (e.g., repair)	☒	☐	☐	☐
In other places, where?:	☐	☐	☐	☒

5. What are the features of the process and environment?		
What is the level of human oversight?	Authentication without human oversight, check has to be completely automated ☐	Check is done by a person who uses the authentication device ☒
If check is done on a conveyor, how fast does the conveyor move?		
How much metal is in the product or environment?		
How much organic/liquid is in the product or environment?		
Are the items to be read in close proximity to each other, to metal,		

etc.?				
Are the items to be read in random orientation?	Yes ☐	No ☒	Don't know ☐	
Are the readers to be handheld, portable, or fixed? (select all that is required)	Portable ☒	Handheld ☒	Fixed ☒	Don't know ☐
Does the system have to work in offline mode, without network connection?	Yes ☐	No ☒	Don't know ☐	

6. What are the requirements regarding performance?	
Read range required (max)	
No. of products to be checked per second	

7. What is the required output format of the authentication system? (select what is required)		
Output must clearly state authentic / not.	☒	
The output has to present suspicious/unclear cases for example by displaying the level of confidence (e.g., *medium confidence*, or 66%), when possible.	☐	
Output has to display also other information to facilitate a further physical / manual product check.	☒	If yes, what information?
Other, what?		

8. Other questions: (leave open if answer is unknown or question is not relevant)	
Where and by whom will the security labels be affixed? E.g., production line (beginning/end);	
What constraints are there for integration of the security feature? (e.g., material, space available)	
Is there a preferred integration method: adhesive, special covering,	

aesthetic covering, integrated invisibly into packaging	
What is the required life-time of the security feature?	
What environmental constraints are there for the security feature (e.g., temperature, pressure, robustness etc.)	
Can the security feature be visible, if also visible feature is secure enough?	
Are there any special requirements regarding tampering resistance?	

5.3 Appendix III: IC Memory

The following table shows the IC memory arrangement of the data and how the data will be organized. A Block is 1 kilobit long, or 170 6-bit ASCII characters.

Description of memory	***Block Numbers***	
Component Mfgr's Birth Record #1	Block 0	Birth Recor #1
Component Mfgr's Birth Record #2	Block 1	Birth Recor #2
Component Mfgr's Birth Record #3	Block 2	Birth Recor #3
Key data that constituates most current value	Block 3	Current Data Record #1
Key data that constituates most current value	Block 4	Current Data Record #2
An open comment area for mechanics to use	Block 5-7	Mechanics Scratchpad area
1st Traceability Maint. Event – eg installed	Block 8	1st Maintenance Event
Etc. – removed	Block 9	2nd Maintenance Event
Etc.	Block 10 -54	X Maintenance Event
Etc. + warning that memory is getting full	Block 55	Next Event + 1st Warning
Etc. + more warnings to change data plata	Block 56 – 58	Next Event + another warning
Etc + last recors & plate must be replaced	Block 59	Next Record + memory filled up
Chip mfgr Memory Control	Block 60 – 63	Belong to Chip mfgr