



Project IST-034144: SToP
Stop Tampering of Products

Deliverable 5.1

Implementation roadmap, specific requirements, and design of first integrated lab trials

Leading Partner: Spacecode

Security Classification: Public (PU)

November 2007

Version 1.0

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

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)	Eric Gout (SPC), Harald Vogt (SAP)		
Responsible Author (Partner)	Eric Gout (SPC)	E-mail	Eric.gout@spacecode-rfid.com
		Phone	{ Phone }

Version History

Version	Date	Description	Author
0.1	07-10-15	Compilation of material	EG
1.0	07-11-08	Final Formatting and submission	MS

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

Table of Contents

Project Details	I
Version History	I
Table of Contents	II
Table of Figures	III
Table of Tables.....	III
Executive Summary	1
1 Overview	2
2 PVI.....	3
3 Aviation Industry	4
3.1 Description	4
3.2 Trial Components.....	6
3.2.1 Secure Part History.....	6
3.2.2 Mobile Reader Device.....	6
3.2.3 Authentication.....	7
3.2.4 Synchronisation.....	8
3.3 Resources.....	8
3.4 Implementation Plan	8
4 Luxury Goods Industry	10
4.1 Description	10
4.2 Trial Components.....	11
4.2.1 Tag Integration in Metallic Environment	11
4.2.2 Tag Integration in Leather Environment	12
4.2.3 Hardware/software integration.....	12
4.2.4 Basic RFID Authentication.....	12
4.2.5 Data Capture	13
4.3 Implementation Plan	13
5 Pharmaceutical Industry.....	15
5.1 Trial Goals	15
5.2 Simulated Supply Chain.....	17
5.3 Process Description.....	17
5.4 Required PVI Functionality.....	19
5.5 Resources.....	19
5.6 Implementation Plan	19
6 References	21

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

Table of Figures

Figure 1: Lifecycle of an LRU 5
Figure 2: RFID Data Layout 6
Figure 3: Trial roadmap for tags in metallic environment.....11
Figure 4: Tag integration in leather environment12
Figure 5 - Flow of goods in the pharmaceuticals supply chain17

Table of Tables

Table 1: Luxury goods authentication objectives10

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

Executive Summary

This document outlines the planning of practical trials that will be carried out during the lifetime of the SToP project. The goals of these trials are to prove the applicability of RFID tags on difficult products; the feasibility of combined security features; the execution of work processes related to product authentication in (near) real-world settings; establish software support for product authentication processes. The outcomes of these trials will heavily influence the preparation of application guidelines (deliverable D5.4).

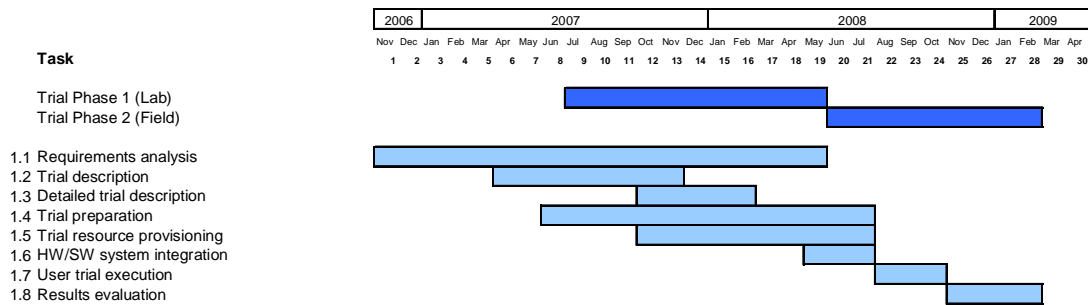
The trials will be executed in two phases. The first phase (lab trial phase) will ensure the operability and functional correctness of all sub-systems. This includes the used tagging technologies (including RFID), the user devices, and the background software system. The second phase (field trial phase) covers the usage of this infrastructure in (near) real-world settings, walking through practically significant use cases, and involving expert users and field personnel.

A detailed task plan has been worked out for the preparation and execution of the trials. Three industry-specific trials are anticipated, for each of which a plan is laid out in this document. The individual trials are aligned in an umbrella planning that ensures that project resources are efficiently employed. The planning for the second trial phase is subject to further refinements such that results of the first phase can be appropriately taken into consideration.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

1 Overview

The SToP trials will be executed in two main phases: a lab trial phase and a field trial phase. The lab trials will ensure the functional correctness and the operability of all involved system components. These trials have started with early preparations of RFID tags for harsh environments (in June 2007) and will last approximately until May 2008. Building on the experiences from this first phase, the second phase will be prepared such that practical execution “in the field” can start in May 2008. The following chart shows the scheduling of the trial phases and the associated high-level tasks.



This chart shows the general tasks for trial execution, which will be detailed later in this document according to the industry-specific trials. The tasks are commented in the following table, including their connection to the project goals:

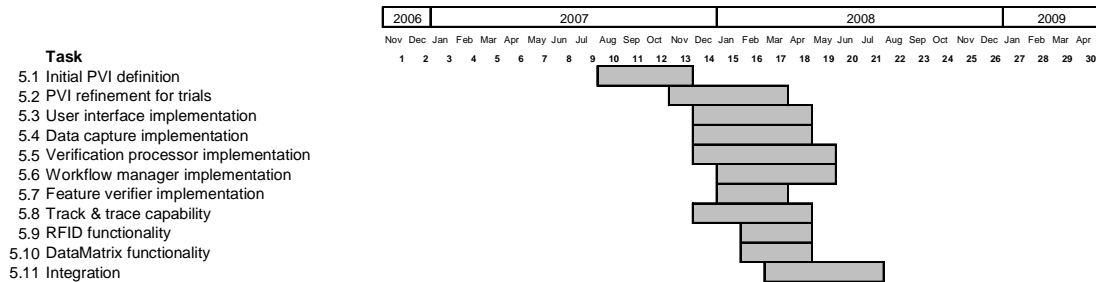
Task #	Description
1	Ongoing requirements analysis, taking experiences from lab trials into account; providing input for deliverables D1.2 and D5.2
2	Preliminary description of trial design and goals; mainly used for internal communication and planning
3	Detailed description of trial design and goals; part of deliverable D5.2
4	All preparatory tasks for trial execution, such as resource planning and user training
5	Resource provisioning, ensuring within the participating organizations that preconditions for trial execution are fulfilled
6	Technical integration of all involved systems; ensuring operability and correctness
7	Execution of practical field trials (corresponding to D5.3)
8	Evaluation of trial results; providing input for D5.4

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

2 PVI

The Product Verification Infrastructure (PVI) is an integral component for the SToP. The PVI will be used to provide the information processing framework used for executing the product authentication trials.

The following implementation roadmap ensures that all PVI modules required for executing the trials will be available when the trials start. The architecture and the functionality of the PVI are described in document D3.2, “Definition of Product Verification Infrastructure”. Here, we briefly sketch the tasks required for the PVI implementation in order to facilitate alignment with the application trial execution.



Task #	Description	Responsibility
1	Definition of the PVI; functional and modular specification (D3.2, D3.3)	SAP, ORIA
2	Ongoing refinement according to emerging trial requirements	SAP, ORIA
3	User interfaces targeted at involved user groups	SAP, ORIA
4	Data capture for various security features and linkage to product master data	SAP, ORIA
5	Verification processor, which is steering the verification process	SAP, ORIA
6	Workflow manager as the central process control	SAP, ORIA
7	Information processing for relevant features	SAP, ORIA
8	Track & trace functionality as related to product authentication	SAP, ORIA
9	Information processing for supporting RFID	SAP, ORIA
10	Information processing for supporting DataMatrix codes	SAP, ORIA
11	Integration with system components (D3.3, D3.4)	SAP, ORIA

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

3 Aviation Industry

The aviation industry is threatened by the problem of suspected unapproved parts (SUP). A suspected unapproved part is an aviation part (a part, device, or material that is used in the production process of an aircraft) which is assumed not to meet the requirements of an approved aviation part. The presence of an SUP seriously violates the security standards of an aircraft and thus represents a critical threat to passenger safety. Characteristics that give rise to doubts about the airworthiness of an aviation part are outdated or incomplete accompanying documents. SUPs do not necessarily have to be faked parts. For example, there have been cases where original aviation parts have been removed from scrapped airplanes and reinserted into the licit supply chain.

The aviation industry has the vision to solve this problem at least on the level of line replaceable units (LRU). These are closed groups of aviation parts that have to be replaced during the lifecycle of an aircraft. **The goal of the industry is to have an electronic pedigree for each LRU that documents its origin and its lifecycle.** Currently, the Air Transport Association is working on the next version of Spec 2000 Chapter 9-5 that deals with radio frequency identification on parts where the format of pedigrees is being specified [ATA07].

The goals of the aviation specific lab trials are:

- Ensure the feasibility of an RFID tag based data storage of LRU historical data. This includes the reliability of tag reading during interaction with a mobile device.
- Ensure that in a mobile working environment, historical data can be written to tags and correctly signed. Here, the usability of the system is in the focus of attention.
- Ensure that data authentication yields safe results, i.e. correctly signed records are successfully authenticated while incomplete or damaged entries are rejected.
- Ensure the correct operation of the synchronisation procedure between tags and the central database.

3.1 Description

To enable electronic pedigrees for parts the aviation industry envisions a solution that consists of the following building blocks (see Figure 1):

- Setup of a central aviation part registry – birth and lifecycle data (unique manufacturer ID, unique part ID, event type, context information, relevant application data, etc.) of aviation parts will be stored within a central database that is only accessible by authorised parties.
- Equipment of LRUs with high frequency RFID tags – the aviation industry wants to provide access to crucial data associated with aviation parts at any time and anywhere. As access to the central database might not be possible at all times, all relevant information needs to be carried along with the aviation part itself as well. For this reason, LRUs will be equipped with high frequency RFID tags containing 64 kbit of memory that will include the relevant birth

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

and lifecycle data, which will have to be digitally signed to ensure their integrity. If a network connection is available while a new record is being created, the database and the content of the RFID tag will be updated at the same time. If not, the database has to be synchronised on reconnect.

- Update of lifecycle data in case of safety critical events – in case of safety critical events, e.g., a modification of an aviation part, the database and the content of the RFID tag will have to be updated accordingly. Storing this data within two different locations also provides a way to detect cloned RFID tags when tag and back-end entries are updated and synchronised after all interactions.
- Data security - the history information stored in the central database as well as on RFID tags must be secure against tampering. It has to be ensured that only authorized parties are able to create new records, or access certain information. Historical information must be digitally signed in order to protect it against manipulation and to ensure the authenticity of the data.
- Tag security - the tag must authenticate itself to a reader device, e.g., by means of challenge-response authentication. As the secret key within the RFID tag is hard to access, this technique protects tags against cloning.

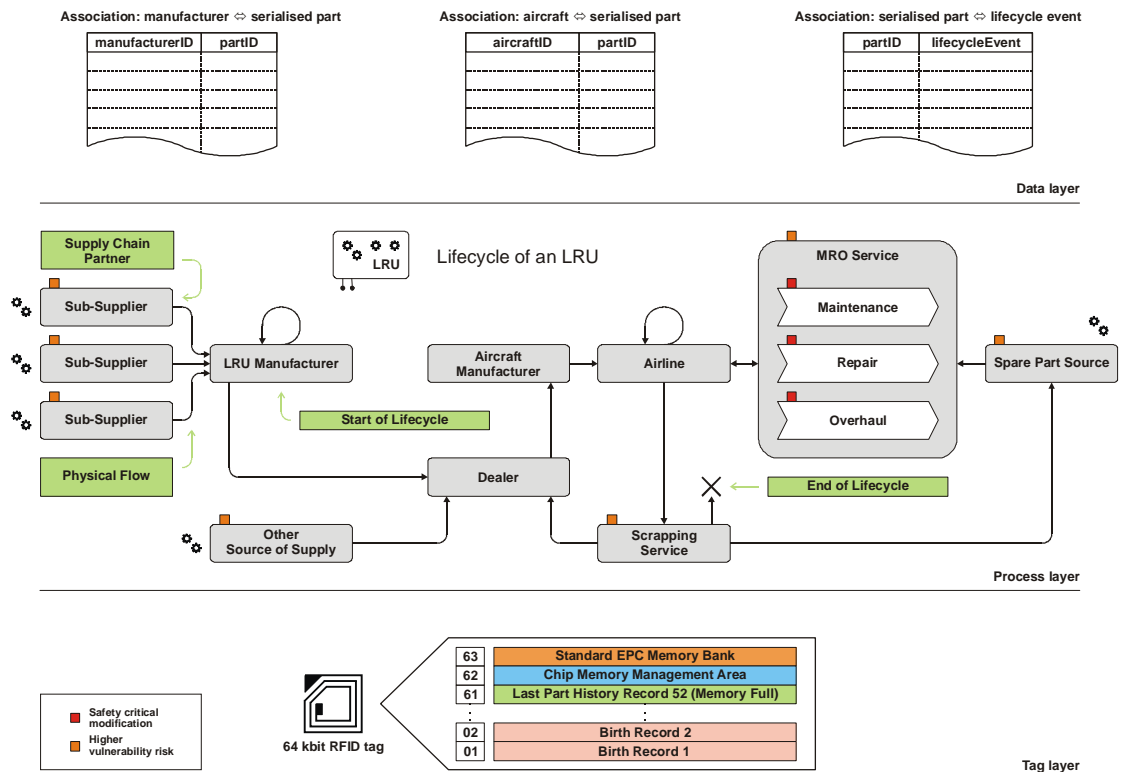


Figure 1: Lifecycle of an LRU

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

3.2 Trial Components

3.2.1 Secure Part History

The part history section on an RFID tag for aviation parts will be specified in the (not near) future by the Air Transport Association as part of Spec 2000 Chapter 9-5. The SToP project will already investigate a possible concept to show the overall feasibility although we will adhere to the tag data layout that has been specified by the ATA so far. These are the two first blocks as depicted in Figure 2. The other blocks have been specified only in terms of their location within memory.

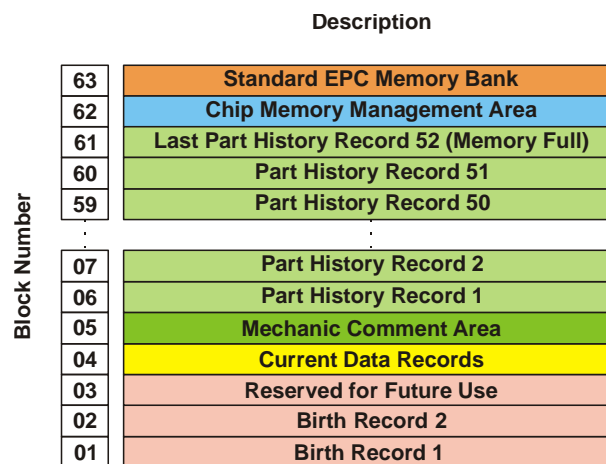


Figure 2: RFID Data Layout

Within the change request to Spec 2000 Chapter 9-5 [ATA07] only the data format of birth data is proposed. The birth data section contains information such as manufacturer data and the unique serial number of an aviation part. Although the memory position for part history records is already specified, it is still unclear which data will be stored within these records and how it will be structured. Therefore we will come up with a proposal for the content and its structure.

As outlined above one of the requirements of the industry is to ensure the integrity of the part history records by digital signatures. The size of every block is 1000 bit = 125 byte. Due to this constraint certain algorithms for public-key cryptography like RSA cannot be used as they require too much memory. For the trial we therefore will have to have a look at alternative approaches like elliptic curve cryptography that need less memory but still offer a comparable security level. The tasks for this goal will include:

- Development of a data layout for part history records
- Development of a security concept to protect these records from tampering

3.2.2 Mobile Reader Device

It will have to be possible to authenticate LRUs not only at special terminals but also with mobile reader devices. For this reason the SToP project will develop a GUI application for such a device that will be capable of viewing all relevant information on a display limited in size. The application will have to work both with and without

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

network connectivity, although in the latter case it will not be possible to detect cloned RFID tags.

As only authorised users are allowed to create and authenticate digital signatures, they have to be stored in a secure environment. To this end we plan to come up with a solution involving secure smart cards that are needed to operate a mobile reader device.

The software of the reader device will have to include the following functionality:

- Reading (pedigree) records from RFID tags and displaying them in a user-friendly way
- Writing (pedigree) records on RFID tags (As network connection might not be available at that point in time, the private key to sign the records would have to be stored on the mobile reader device. For security reasons this key would have to be protected, e.g., by storing it within a smart card.)
- Authenticating (pedigree) records without network connectivity (In this case only digital signatures of pedigree records are verified. This requires that records contain the public key of the signer. In addition, the public key of the certificate authority that has signed this certificate (and all other certificates to verify the certificate path) has to be stored on mobile reader devices.)
- Authenticating (pedigree) records with network connectivity (In this case the records on the RFID tag are also compared to the ones in the database.)
- Synchronising data on RFID tags with the remote database (In this case records were written on the RFID tag when there was no network connection available.)

3.2.3 Authentication

As outlined above, authentication of LRUs will have to be possible both with and without network connectivity. In case no network connectivity is available all digital signatures stored on the RFID tag have to be verified. In case of an existent network connection all records stored on the tag are also compared with the ones stored within the central database. This protects the system from duplicates as the records stored on the tag and the ones stored within the central database most likely differ from each other if the content of an RFID tag was copied to another one. It is highly important that this protocol has to be implemented as efficient as possible. The secure solution also requires development of an identity management and key distribution system.

The protocol necessary to authenticate history records stored on an RFID tag are defined. Firstly, all history records on the tag are read and authenticated by the mobile reader device, i.e. their digital signatures are verified. If network connectivity is available, the history records are also compared with the ones within the central database to detect cloned tags (a clear indicator for a cloned tag is if it contains less history records than the central database). If network connectivity is available, missing history records within the central database are then synchronised (see below).

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

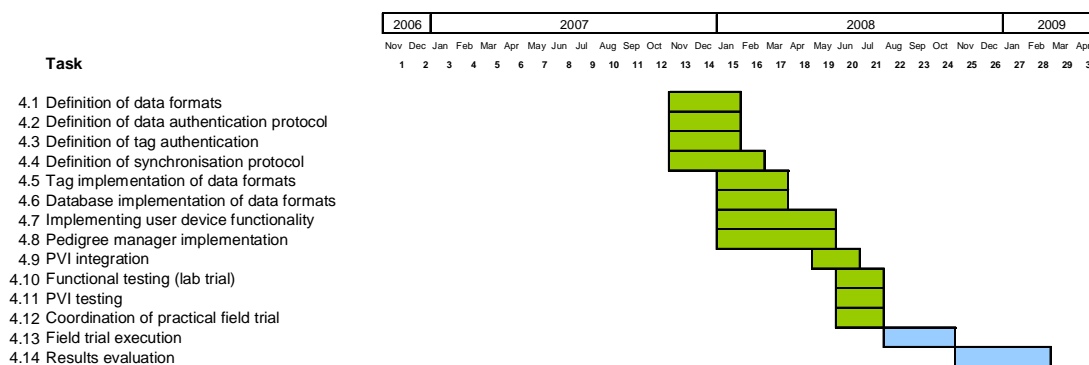
3.2.4 Synchronisation

This task will elaborate the steps necessary to synchronise the history records stored within the central database and on an RFID tag. In case of an update or synchronisation of history records (stored on a tag) with the help of a mobile reader device, these history records have to be synchronised with the central database. This involves detecting history records that are stored on the tag but not within the central database.

3.3 Resources

- Tags: 20 pieces
- Readers: Bluetooth pens, tablet PCs

3.4 Implementation Plan



Task #	Description	Responsibility
1	Definition of a data format for history records on RFID tags and a database schema for the back-end system	AD
2	Definition of a protocol to authenticate a pedigree stored on an RFID tag including communication with the PVI in the back-end system	AD
3	Definition of a protocol to authenticate an RFID tag	AD
4	Definition of a protocol to synchronise a pedigree stored on an RFID tag with the corresponding one stored within the PVI	AD
5	Tag implementation of data formats	AD
6	Database implementation of data formats	AD
7	Implementation of software for mobile reader devices used for authentication	AD
8	Implementation of the PVI module supporting authentication and synchronisation of electronic	SAP, ORIA

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

	pedigrees	
9	Integration of software for the mobile reader device with the PVI in the back-end system	SAP, ORIA
10	Lab testing of devices	SAP, AD, ORIA
11	Lab testing of the PVI	SAP
12	Preparation of field trial	AD
13	Field trial that involves testing of the whole system according to the goals in a realistic environment (e.g., in a test rig)	AD, SAP, ORIA
14	Evaluation of results gained from field trial	HSG

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

4 Luxury Goods Industry

In this industry, it should be possible to perform product authentication at various locations within the supply chain. This should be possible with various features using methods that are simple to use, cost-effective to implement, and that yield quick results.

4.1 Description

The objectives of the SToP trials are to demonstrate the feasibility of an effective and efficient authentication process for two different types of products.

Table 1 gives an overview of the constraints and specific objectives of the product types. The goal of the lab trial is to establish the integration of suitable security tags in these types of products and to test the feasibility and speed of various authentication methods.

Table 1: Luxury goods authentication objectives

Authentication requirements	
Metallic products	Soft goods
Tag integration constraints	
Very small available space Metallic environment Security tags integrated in assembly line Only ID number should be visible	Soft and small security tag Security set-up after assembly Only ID number should be visible
Initial security requirements	
High level of security “Natural” features to be considered Management of multiple (combined) security features	High level of security
Authentication objectives	
Authentication of one object at a time Reading in arbitrary orientation Items may be close to each other One or more manual steps Best response time to be found	Authentication of single and multiple objects at the same time Random orientation Authentication shall be possible without human oversight Automatic procedure

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

As illustrated in Table 1, the main challenge for the lab trials is to demonstrate the successful integration of tags into products, particularly in a metallic environment. The integrated tags must be readable, possibly writeable and able to successfully participate in authentication. Reading devices will have to communicate with the tags as well as with the PVI.

Product authentication throughout the supply chain involves different user groups that need to be addressed. These user groups perform product authentication in different contexts, and they differ in the level of access they have to the PVI. The following user groups have been identified to be relevant in the luxury goods area:

- Anti-counterfeiting team, requires overall visibility
- Brand headquarter for the specific brand, product category managers
- Internal retailers, boutique staff and service centers
- Authorized retailers and external service providers
- Customs and external investigators
- Customers

Although the user role specific interaction with the PVI will be tested in the field trials, the selection of authentication approaches and devices already has to take the different user groups into account.

4.2 Trial Components

4.2.1 Tag Integration in Metallic Environment

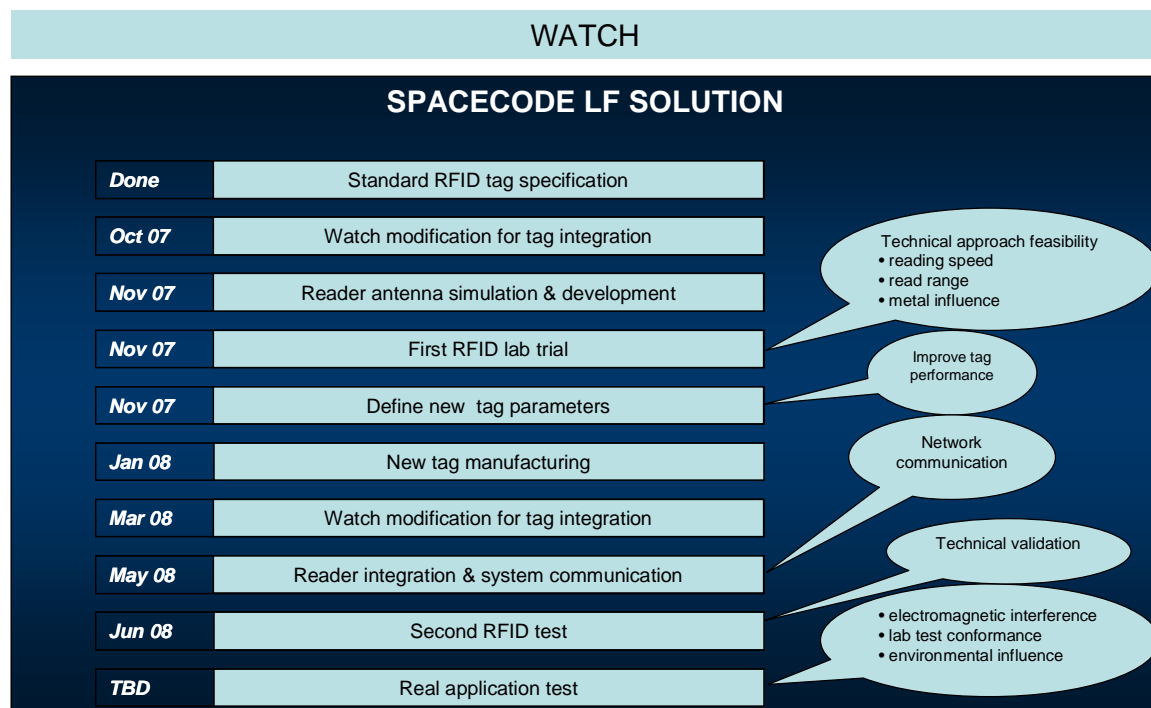


Figure 3: Trial roadmap for tags in metallic environment

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

4.2.2 Tag Integration in Leather Environment

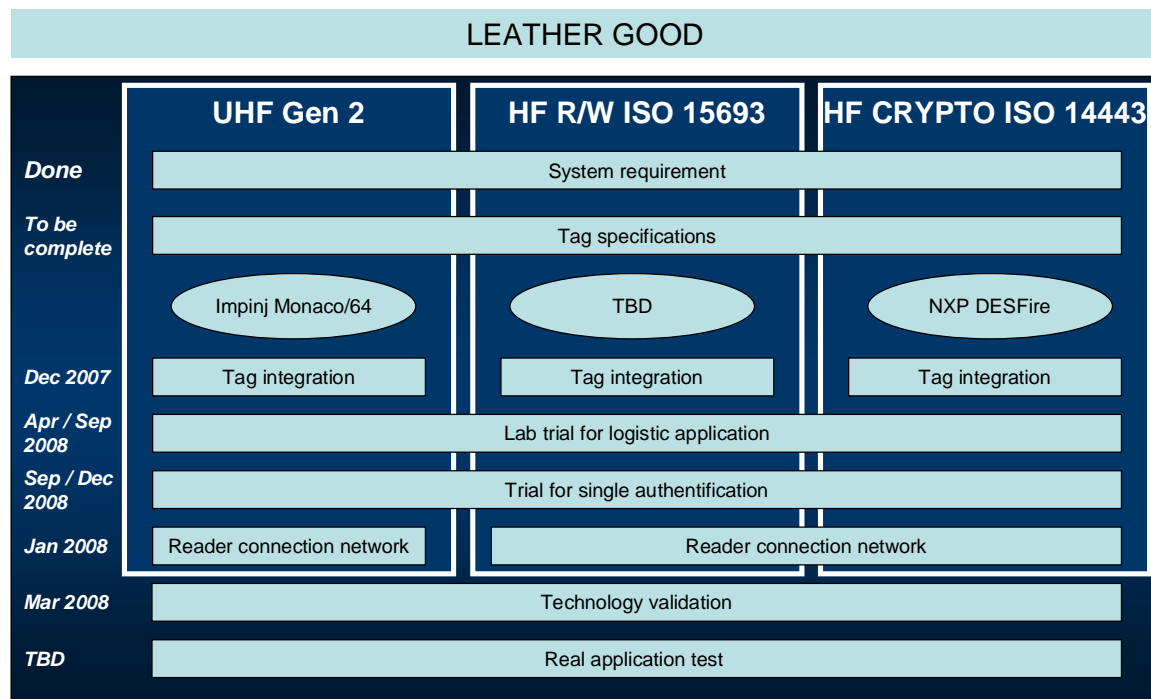


Figure 4: Tag integration in leather environment

4.2.3 Hardware/software integration

The goal of hardware / software integration is to test and demonstrate the interaction between the hardware, more specifically the reading devices, and the PVI.

The first task is therefore to select reading devices that are capable of performing the desired authentication approaches, e.g., RFID readers that communicate with tags or reading devices that capture directly product properties. In case of RFID readers, it needs to be determined whether the same reader can be used for metallic goods as well as for leather goods. The integration tests will be performed for each reading device.

During the trial, it will be demonstrated that the reading device can communicate with the PVI. In the reading test, it will be demonstrated that data can be sent from the device to the PVI or that the PVI has access to the data captured by the device. For some devices like RFID readers, it will also be possible to write data. For these devices, it will also be demonstrated that data can be passed on from the PVI to the device.

4.2.4 Basic RFID Authentication

The goal of this task is to test basic authentication methods based on RFID tags. The trial will involve various authentication methods that require cryptographic, read/write or read-only functionality from the tags. The trial will not cover track and trace based authentication methods beyond serial number verification, but will concentrate on feature-based authentication. The trial will focus on the basic authentication functionality and will not cover additional functionality of the PVI like access control

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

or incident management. Before running the trial, the authentication protocols will be designed and implemented.

The trial will be performed with raw RFID tags or dummy products (one metallic product and one leather good). The goal of the trial is to demonstrate that the authentication method can distinguish correctly between genuine and counterfeit products in a controlled lab environment. Simulated original and counterfeit products will be tested to produce positive and negative authentication results. Furthermore, the time needed to perform the authentication will be measured.

4.2.5 Data Capture

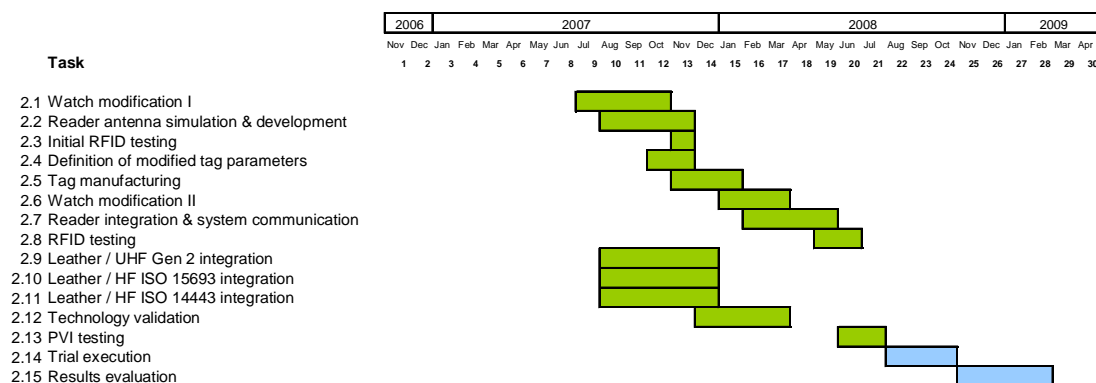
The goal of the data capture trial is to test some of the functionality of the Feature Data Capturer Module specified in deliverable D3.2. The Feature Data Capturer ensures that the data needed for feature-based authentication, e.g., cryptographic keys or serial numbers, is stored in the database. Unlike the software/hardware integration test, which demonstrates the communication between reading devices and the PVI, the data capture trial also involves database operations.

The data capture trial will be performed with the same tags or dummy products (metallic products/leather goods) that are used for the basic authentication trial. The data capture trial will comprise the following tasks:

- Feature writing (if applicable): A feature created by the PVI (e.g. a serial number) will be written to the tag and at the same time stored in the PVI feature database as a reference value for subsequent authentication
- Feature reading: One or multiple values will be read from the tag and stored in the PVI feature database.
- Verification: In order to ensure that correct values were written or read, an authentication will be performed

In this trial, the feasibility of feature writing and feature capturing will be demonstrated. With a limited number of tags or dummy products the reliability of the data capturing and data writing process will be tested, i.e. how many features are not written or captured correctly at the first try. Writing and reading times may be measured.

4.3 Implementation Plan



Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

Task #	Description	Responsibility
1	First watch modification	SPC
2	Reader antenna simulation and development	SPC
3	Initial RFID testing	SPC
4	Definition of modified tag parameters	SPC
5	Tag manufacturing	SPC
6	Watch modification, 2 nd phase	SPC
7	Reader integration and system communication	SPC, SAP, ORIA
8	RFID testing	SPC
9	Leather / UHF Gen 2 integration	SPC
10	Leather / HF ISO 15693 integration	SPC
11	Leather / HF ISO 14443 integration	SPC
12	Technology validation	SPC
13	PVI testing	SAP, SPC
14	Field trial execution	RM
15	Results evaluation	HSG, RM

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

5 Pharmaceutical Industry

We plan to perform a trial within SToP that demonstrates product authentication in the pharma industry. The aspired result is the demonstration of an operational “product verification infrastructure” consisting of tagged goods, devices and procedures to verify the authenticity of items, and a software system that supports the related information processing. The general objective of product authentication is to reliably distinguish original items from counterfeit items.

The trial will be performed in two phases: an initial lab test where the full functionality and all procedures are executed; and an extended test with more varied parameters.

1. The initial lab test will make sure that all subsystems are operational and that the defined working procedures provide full support to the relevant business processes.
2. The extended test will evaluate the complete system in various operational conditions on a wider scale, for example regarding the number of users.

Before the trial begins, we will acquire drug packages that represent both authentic and fake drugs. The trial will take place in a simulated pharma supply chain. During the trial, fake packages will be injected into weak points in the supply chain. Authentication will take place in several points in the simulated supply chain.

5.1 Trial Goals

The goals of both trials are:

1. Verifying the usability of the hardware operations.
 - a. RFID tags and 2D barcodes can be read within reasonable time.
 - b. The data and technology is reliable.
2. Verifying the intended operations of the PVI. This includes:
 - a. Correctly detecting whether products are authentic or fake.
 - b. Correctly detecting whether products are diverted.
 - c. Correctly determining the trace that a product took in order to facilitate backward logistics.
3. Testing the performance of the PVI:
 - a. Response time.
 - b. Accessibility, completeness, and relevance of information.
 - c. Usability.
 - d. Trust in the results of the system.
4. Identifying the experiences learnt regarding the integration of relevant work procedures. This can result in a “best practices” guideline that summarizes the most important experiences and lessons learnt.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

The following measures are going to be used in order to evaluate the achievements:

Goal	Measure	Comment
Hardware response time	Average read time during authentication, measured over a sample set	We expect an average read time of at most 2 seconds.
Reliability of data	Count missed reads and erroneous data received	We expect a certain amount of read misses, but not incomplete or wrong data
Distinguish between original items and fakes	False negative, false positive rates	Since we are not dealing with real-world counterfeiters, the results here are biased
Detect product diversions	Inject data that provides evidence for a diversion; detect & report this fact to the user	What information is required? (What should be displayed to the user, how can a diversion be detected?)
Provide an item trace	Inject item trace data; display to user	Again: what information is relevant?
System response time	Average time from verification start to final result	Multiple/combined features may be interesting here.
Accessibility of information	How fast can the user retrieve the relevant information?	
Completeness of information	In how many cases does the user not get the relevant information for the task at hand?	
Relevance of information	Determine the minimal set of data to be used	
Usability	Count number of wrong interactions, missed information, time to get familiar with the interface and the concepts behind the system	Use a question sheet to ask the users about it
Trust in the system	User rating of trust.	What are appropriate measures of trust?
Work procedures	Identify work procedures that are adjacent to the authentication procedure in different contexts	Context could vary: pharmacy, storage house, production line ...

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

5.2 Simulated Supply Chain

Figure 5 depicts the pharma supply chain, showing where items can be tracked and authenticated.

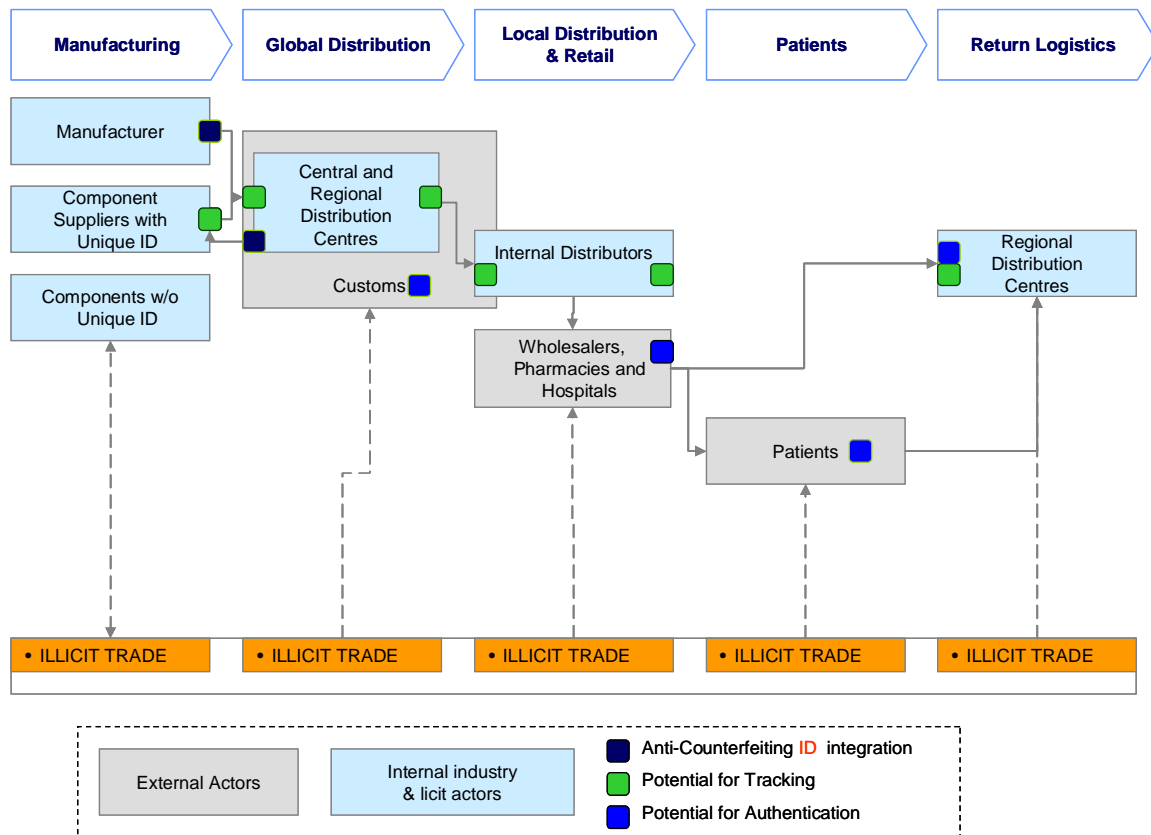


Figure 5 - Flow of goods in the pharmaceuticals supply chain

In the trial, we will simulate a simple supply chain based on the one above, comprising:

- 1 Manufacturer
- 1 Distribution Center
- 1 Customs location
- 2 Wholesalers
- 2 Pharmacies

5.3 Process Description

The following processes will occur in the trial:

1. **At manufacturing:** Forty pharmaceutical packages of two different SKUs will be registered in the PVI. Their unique numbers will be stored along with the features that will be used in authentication. Also, the intended selling location will be set in the PVI. This procedure will be carried out manually or semi-automatic.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

2. **Shipping:** The work procedures for aggregating and shipping items will be described. The relevant elements will be identified that are required for item authentication integration.
3. **Tracking at the Distribution Center:** The packages will be read at the inbound dock of the Distribution Center and the combination of the item and location will be recorded in the PVI.
4. **Shipping through customs:** Items are to be shipped to two different wholesalers, one of which is in a different country thus requiring passing through customs. The relevant work procedures, with item authentication, will be identified.
5. **At customs:** Five authentic packages will be replaced by fake packages right before customs. Only a handful of packages will be checked by customs for the possibility of being counterfeits because of limited customs resources. The PVI will help determine how many packages should be checked, which packages are to be checked, and when would we have reached a satisfactory level of confidence that no fake packages are encountered.
6. **At the wholesalers:** Samples of the received products will be authenticated, so any fake package that was not detected by customs should be detected at the wholesalers. The authentication process results in the automatic tracking of the products.
7. **Shipping to the POS:** The products are shipped to a POS in the same country, thus not passing through customs. Again, five authentic packages are replaced by fake ones between the wholesaler and the POS.
8. **At the POS:** A last authenticity check takes place at the POS. Also, as the product is being sold, a check is made to check for product diversion.
9. **Incidence response:** Back-office workers are informed about incidents, i.e. failed authentication attempts. Determine the relevant work procedures.
10. **Return logistics:** The manufacturer should be able to receive the full pedigree/ trace of the individual partner once it is returned.

The extended phase is varied according to the following parameters:

Parameter	Extended value	Comment
Number of users	At least two who are trained in actively performing the process	
Location	Actual working environment; different physical locations	The intension here is to provide the test candidate with a familiar environment such that the focus of attention is restricted to the new aspect of item authentication
Embedding in work processes	Adjacency to different process steps	In order to determine the optimal embedding

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

Task #	Description	Responsibility
6	Component integration: PVI, readers	SAP
7	Phase 1 execution: lab tests of infrastructure	SAP, SPC, ORIA
8	Phase 1 evaluation	SAP, SPC; ORIA
9	Provisioning of expert users for field trials	NPH
10	Provisioning of evaluation questionnaires	HSG
11	PVI testing	SAP
12	Trial execution	NPH
13	Results evaluation	HSG

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.1		
Title	Implementation roadmap, specific requirements, and design of first integrated lab trials	Date	2007-11-08

6 References

- [ATA07] ATA (Air Transport Association): Spec 2000 Chapter 9-5 – Radio Frequency Identification on Parts (Change Request Form). January 2007