



Project IST-034144: SToP
Stop Tampering of Products

Deliverable 3.1

Report on relevant state-of-the-art research, existing technologies and products

Leading Partner: SAP

Security Classification: Public (PU)

November 2007

Version 2.0

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	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)	Nina Oertel (SAP), Jens Müller (SAP), Ali Dada (SAP), Felix Graf von Reischach (SAP), Harald Vogt (SAP), Mikko Lehtonen (ETH)		
Responsible Author (Partner)	Nina Oertel (SAP)	E-mail	nina.oertel@sap.com
		Phone	+49 721 6902-19

Version History

Version	Date	Description	Comments
1.0	07-05-03	Final Version	
2.0	07-10-10	Modified version for resubmission	<ul style="list-style-type: none"> - Restructuring for privacy discussion, 2.8 - Addressing scalability and reliability issues, 2.9 - Extended discussion on integrated solutions - Final Formatting and submission

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Table of Contents

Project Details	I
Version History	I
Table of Contents	II
Table of Figures	IV
Table of Tables.....	IV
List of Abbreviations.....	V
Executive Summary	1
1 Introduction	2
1.1 Project Description.....	2
1.2 Objectives of Deliverable 3.1	3
1.3 Relations to Other Tasks, Deliverables, and Work Packages	3
1.4 Document Structure	5
2 Approaches and Methods for Authenticating Products and Securing the Supply Chain.....	6
2.1 Introduction	6
2.2 Identity and Identifiers	7
2.2.1 Identity.....	7
2.2.2 Coding and Numbering schemes	8
2.2.3 Data Carriers	9
2.3 Product Authentication.....	11
2.3.1 Direct Authentication	13
2.3.2 Authentication Based on Difficult to Reproduce Features.....	15
2.3.3 Verification of Unique Identifiers	17
2.3.4 Plausibility Checks of Track and Trace Data	18
2.3.5 Secure Object Authentication	26
2.4 Copy Protection of Tags.....	32
2.5 Binding Between Tag and Product	35
2.6 Sealing Products	36
2.7 Status Verification	38
2.8 Privacy protection	40
2.9 Dependability of Network-Based Approaches	42
2.9.1 Network Performance Risks and Bottlenecks	42
2.9.2 Security.....	44
2.9.3 Business Intelligence and Privacy Issues	45
2.9.4 Discussion.....	45
2.10 Combined Authentication Approaches	45
2.11 Analysis and Comparison.....	46
3 Commercially Available Authentication Infrastructures	49
3.1 Introduction	49
3.2 Products.....	49
3.3 Summary and Analysis of the Available Products	55
4 State of Implementation of Technical Anti-Counterfeiting Measures in Relevant Industries.....	58
4.1 Introduction	58
4.2 Pharmaceutical Industry	58
4.3 Aviation Industry	62
4.4 Luxury Goods Industry	65

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

4.5	Security Document Industry	69
4.6	Analysis	71
5	Conclusion.....	74
	References.....	76

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Table of Figures

Figure 1: Relations to Other Work Packages.....	4
Figure 2: Document Structure.....	5
Figure 3: The Electronic Product Code.....	9
Figure 4: Data Matrix Code with a Symbol Size of 20x20.....	10
Figure 5: Distribution of Description of Authentication Approaches.....	13
Figure 6: Direct Authentication.....	14
Figure 7: Architecture of a System for Verifying Unique Identifiers.....	17
Figure 8: The EPCglobal Network Architecture.....	22
Figure 9: EPCIS and DS.....	24
Figure 10: An Electronic Pedigree.....	25
Figure 11: Tamper-Evident Plastic Wrap.....	37
Figure 12: Lifecycle of an Aircraft.....	63

Table of Tables

Table 1: Approaches to Product Authentication.....	12
Table 2: Authentication Methods and the Importance of Copy Protection for Tags...33	33
Table 3: Comparison of Authentication Methods.....	48
Table 4: State of Implementation in Relevant Industries.....	73

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

List of Abbreviations

AES	Advanced Encryption Standard
ATA	Air Transport Association
CDP	Copy Detection Pattern
CRC	Cyclic Redundancy Check
DDP	Declaration on Design and Performance
DNS	Domain Name Service
DoS	Denial of Service
DOVID	Diffraction Optical Variable Image Device
DS	Discovery Services
EAN	European Article Number
ECC	Elliptic Curve Cryptography
ECPVS	Elliptic Curve Pintsov-Vanstone Signature
EPC	Electronic Product Code
EPCIS	EPC Information Service
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
GTIN	Global Trade Item Number
ISBN	International Standard Book Number
ISTAG	Information Society Technologies Advisory Group
LSA	Laser Surface Authentication
MAC	Message Authentication Code
NDC	National Drug Code
ONS	Object Naming Service
PDMA	Prescription Drug Marketing Act
PKI	Public Key Infrastructure
PRF	Pseudo-Random Function
PRNG	Pseudo-Random Number Generator
PUF	Physical Unclonable Function
PVI	Product Verification Infrastructure
RFID	Radio Frequency Identification
RO	Read-Only
RW	Read/Write

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

SKU Stock Keeping Unit
SUP Suspected Unapproved Part
UHF Ultra-High Frequency
UID Universal Item Identifier
UPC Universal Product Code
URI Uniform Resource Identifier
TC Trusted Centre
TID Transponder ID
WORM Write Once/Read Many
XML Extensible Markup Language

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Executive Summary

The major technical outcome of work package 3 is a system called *Product Verification Infrastructure*. This system will provide mobile and stand-alone applications and devices with proper services and the related data to easily verify the authenticity of products, particularly in the pharmaceutical, luxury goods, aviation, and security document industries.

This report describes approaches and methods for authenticating products and securing the supply chain. It includes a review and comparison of authentication techniques, comprising direct authentication, authentication by means of a difficult to reproduce feature, verification of unique identifiers, plausibility checks of track and trace data and secure object authentication enabled by cryptographic methods. We conclude that there are two classes of authentication methods: some methods are reliable but costly and slow, while others (particularly the check of track and trace data) are well suited for bulk checking, but not as secure. We furthermore emphasise that plain authentication has to be complemented by additional measures to be truly secure, so methods for protecting tags against cloning as well as methods for ensuring the binding between a tag and a product, integrity protection of packages, and status verification of products are also covered.

In addition, the report will give an overview of commercially available authentication solutions and the state of implementation of technical anti-counterfeiting measures in industries that are of particular interest to the SToP project. The analysis of the state of implementation shows that emerging anti-counterfeiting technologies are adopted slowly and that the fight against counterfeiting by employing technical measures may still be improved. This report will serve as a base for the upcoming design of the Product Verification Infrastructure.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

1 Introduction

1.1 Project Description

The markets for counterfeit products are growing worldwide, comprising virtually all industry sectors from security documents, plane spare parts, and pharmaceuticals to luxury goods. This damages the reputation of brand owners, produces economic losses, promotes inferior working conditions, and puts the safety and health of consumers at risk. Brand owners, health and customs offices use various legal and technical tools to combat grey markets and illicit trade with counterfeit products. One promising approach is the use of Radio Frequency Identification (RFID) technology for tagging individual products and packages, thereby enabling reliable, immediate product authentication and a close integration into enterprise software systems.

The SToP project will develop secure, comprehensive, usable, cost effective, and convenient product authentication mechanisms to help reduce trade with illicit products. The solutions provided will be based on RFID and related ambient intelligence technologies. The technologies employed must be adequate for the specific environments regarding the structure of products and the environments in which they are produced, stored, transported, and traded. Technical obstacles that currently prevent the use of RFID in many areas are targeted as well as the integration of the verification technologies and processes into enterprise system architectures, such as supply chain management systems. Finally, the overall solution must be economically feasible.

Therefore, the main objectives of the SToP project comprise:

- The analysis of the structure, the mechanisms, and the extent of the illicit market and the supply- and demand-side drivers of trade with counterfeit products.
- The development of a business case framework to assist governments and companies (especially small and medium sized enterprises) to calculate the impact of illicit trade on brand name and revenue, the required financial investments, and the return on investment.
- The development of a distributed architecture, enabling enterprises and end-users to efficiently manufacture, deliver and purchase secure and authentic products, comprising
 - the development of smart tagging technologies, and
 - the design of collaborative software components.
- The development of integration concepts helping organisations to seamlessly integrate solutions into their products as well as their business process landscape.
- The implementation of real-world application trials to assess and verify the applicability of the approved solutions.

The SToP project is a publicly funded research project within the European Commission's 6th Framework Programme. The international research consortium is lead by SAP and includes Hochschule St. Gallen, Oria Computers, Spacecode,

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Airbus, and Bundesdruckerei as well as companies from the pharmaceutical and luxury goods industry. The consortium members provide substantial knowledge in the areas of RFID product integration, product tracking, economical issues of counterfeiting, and enterprise processes. The project started in November 2006 and ends in May 2009. Besides a thorough requirements analysis, the development of a product verification infrastructure and the elaboration of economic models, extensive trials to evaluate the proposed solutions will be an important component of the project.

1.2 Objectives of Deliverable 3.1

Deliverable 3.1 is the first report generated in work package 3 which deals with the development of the product verification infrastructure (PVI). The main focus of this work package lies on software related research; its major technical outcome will be the PVI which will provide mobile and also stand-alone applications and devices with proper services and the related data to easily verify the authenticity of products. One objective of work package 3 is to scrutinise state-of-the-art approaches that utilise ambient intelligence technologies to support secure product authentication. The term *ambient intelligence* was coined by the Information Society Technologies Advisory Group (ISTAG) to the European Commission.¹ It is defined as the convergence of ubiquitous computing, ubiquitous communication, and interfaces adapting to the user. Therefore, in the context of product authentication and supply chain security, ambient intelligence-based approaches comprise all methods that utilise the capabilities of tagged real-world objects to store information and to communicate this data.

Task 3.1 of work package 3 is concerned with performing an analysis of the state-of-the-art on ambient intelligence-based approaches for secure product authentication. The aim is to evaluate existing approaches that are used today in industry as well as to survey emerging concepts that support secure product authentication with a focus on mobile and standalone approaches. Also different track and trace methods (e.g. RFID vs. 2D barcodes) will be analysed and compared and their applicability in specific domains will be considered. As also barcodes shall be considered, it is evident that the technologies and approaches presented in this report are not limited to RFID or digital data storage. Other relevant technologies, e.g., the use of 2D barcodes that enable mass serialisation, will also be examined. The results of task 3.1 are directly reflected in this report which details the relevant state-of-the-art research, existing technologies, and products.

1.3 Relations to Other Tasks, Deliverables, and Work Packages

Deliverable 3.1 will create the foundation for the subsequent work carried out in work package 3. By scrutinising existing as well as proposed product authentication systems, this deliverable will present current best-practices and remaining gaps in the area of product authentication. Task 3.2 – the definition of relevant product authentication information and data models – and task 3.3 – the development of security concepts – will benefit from the insights gained. Deliverable 3.1 will pinpoint the strengths and shortcomings of existing authentication concepts and will therefore also contribute to the development of a secure, comprehensive, and easy-to-use PVI.

¹ <http://cordis.europa.eu/ist/istag.htm>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Deliverable 3.1 benefits from the work carried out in task 1.1 of work package 1 – the elaboration of business related and regulatory requirements. The problem analysis relevant for deliverable 3.1 is mainly reflected in deliverable 1.1 – the description of main drivers and mechanisms of illicit trade, the roles of the different licit and illicit actors, and the mechanisms of illicit trade. Deliverable 3.1 provides input for deliverable 1.3 – the description of the status quo of existing technical countermeasures, their benefits and shortcomings. Regarding the problem analysis, we furthermore considered the first results of work package 5 of the BRIDGE project², mainly the anti-counterfeiting problem analysis report.

In addition to that, deliverable 3.1 is closely related to deliverable 4.1, which analyses the state-of-the-art in smart tagging technologies. Deliverable 4.1 focuses on security features (tags) that will be found directly on the product, direct authentication (i.e. authentication based on the natural properties of products), and mechanical sealing technologies. Deliverable 4.1 will also investigate security features that do not make use of electronic components at all. In contrast, deliverable 3.1 will focus on product authentication approaches that utilise product tagging - particularly tags containing an identifier - as well as backend systems containing the decision logic, and will particularly centre on the latter components. Deliverable 3.1 will also investigate electronic sealing. This split between essentially *virtual* concepts (in which security is based on a computational process) covered in deliverable 3.1 and rather *physical* concepts (in which security is based on the manufacturing process) covered in deliverable 4.1 is in accordance with the software related focus of work package 3 and the emphasis on ambient intelligence-based approaches stated in the task description. We included numerous cross-references in both deliverables to point the reader to related sections in the related document.

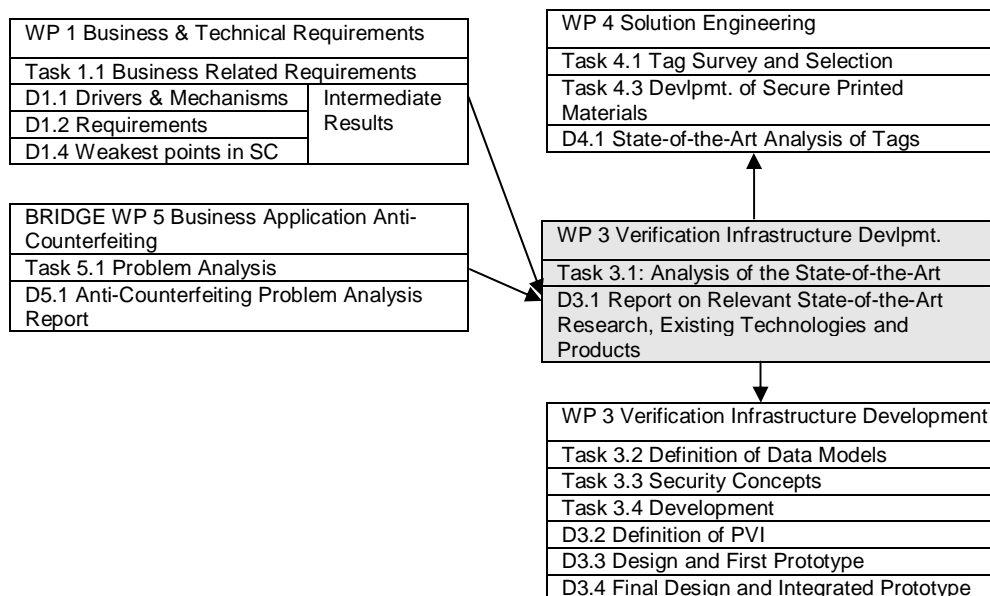


Figure 1: Relations to Other Work Packages

² <http://www.bridge-project.eu/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

1.4 Document Structure

This report presents different aspects of the relevant state-of-the-art, beginning with a survey of fundamental concepts and methods for product authentication, continuing with a review of commercial products, and concluding with a description of the state of implementation of technical anti-counterfeiting measures in various industries.

Chapter 2 describes general approaches and methods for authenticating products and for securing the supply chain. Abstracting from specific implementations and products, we describe and evaluate emerging and proposed generic concepts and technologies. The selection of relevant research is based on an analysis of the threats and vulnerabilities of supply chains. We discuss how products can be identified and authenticated, how tags can be protected against cloning, and how it can be ensured that a tag is bound inseparably to a product. Tamper evidence, the fight against illicit trade (with genuine products), and status checks for ensuring product safety are also covered. We discuss approaches for mitigating privacy concerns, dependability issues of network-based authentication and the combination of various authentication features and approaches.

Chapter 3 presents commercially available applications for product authentication that promise to enhance supply chain security and safety. We classify these products according to the approaches described in chapter 2 and analyse the set of available products in order to identify remaining white spots.

In chapter 4, an overview of the various authentication approaches used today in industries relevant to the SToP project is given. The description of the current situation will reveal areas in which there is room for improvement. Furthermore, the real-life experiences of companies will help to identify authentication approaches that are well suited for certain product, industry, and supply chain types.

The three main chapters of this report will each conclude with a section that analyses, compares, and summarises the main results presented before. Chapter 5 concludes this report by summarising our achievements and by specifying how the results may contribute to the design of the PVI.

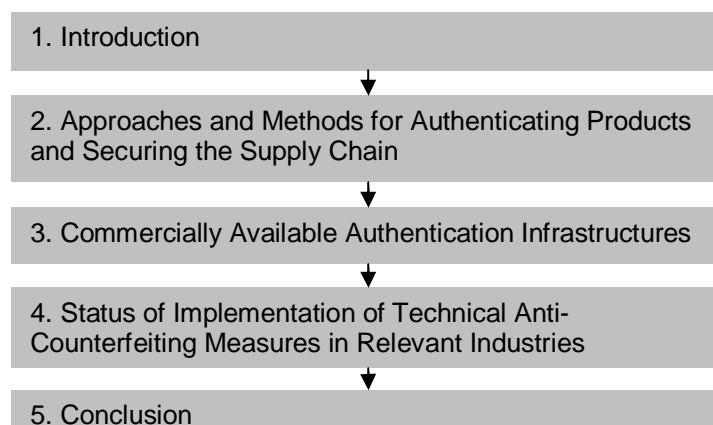


Figure 2: Document Structure

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

2 Approaches and Methods for Authenticating Products and Securing the Supply Chain

2.1 Introduction

In this chapter, we describe relevant research in the area of authentication technologies and product security. We focus on general approaches and methods (these terms are used synonymously in this report), rather than specific products or implementations. We will now motivate which research is relevant in the context of the SToP project and why, we will define the scope of this chapter and outline how this chapter is organised.

As one goal of the SToP project is to enable a secure and efficient product authentication, this chapter focuses mainly on authentication approaches. However, plain authentication has to be complemented by additional safeguards, so that the authentication methods cannot be tricked or circumvented easily. For example, it is useless to employ copy protected RFID tags if they can be ripped off and reused on other (counterfeit) products easily. We therefore based our choice of approaches and methods relevant to the SToP project on an analysis of the possible threats against a supply chain. These threats will be studied in detail in deliverable 1.4 of work package 1 and are briefly described here.

A threat is any action that prevents that safe and genuine products are delivered to the customer through licit distribution channels. Both the customer and the brand owner (or manufacturer) of a product can be negatively impacted by these actions. These threats are a main point of concern for companies and are detailed, e.g., in [PSR04], [Ina06a], and [KSCB03]. They can be grouped into four broad categories:

- Counterfeit products entering the supply chain
- Parallel trade (deviations, grey marketing, parallel imports)
- Tampering of products (e.g., substitution of package contents, refilling, adding of hazardous substances)
- Wrong status of products (e.g. product past its sell-by date)

Counterfeited, tampered, and wrong status products threaten the safety and health of consumers. In contrast, illegally traded genuine products are not a safety threat, but rather impact the revenue of companies, as do counterfeits and possibly also tampered goods. The terms grey marketing, parallel trade and product deviation are used synonymously in this report. However, parallel trade can be legal or illegal, often constituting a breach of contract since products are traded without the consent of the right-holder in the destination market in the latter case. A glossary of related terms can be found in deliverable 1.1.

Product authentication, i.e. the verification of the identity an object claims to have, can either be performed by checking the natural properties of a product or by adding an artificial feature to a product and performing a check based on the properties of this feature. Adding security features provokes various counter-reactions by counterfeiters [LSMF06]: the complete omission of security features, the use of misleading security features (that are sufficiently similar to the real feature to avoid closer inspection), the

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

reuse of security features, or the cloning of security features. Absent or only superficially similar features are easy to spot upon close inspection. However, the reuse and copying of security features present severe threats to supply chain security that need to be guarded against. We will therefore also review approaches that ensure that a tag is not separated from the corresponding product (binding) as well as ways to prevent the cloning and altering of features and data stored on tags. This includes the copy-protection of RFID tags as well as protecting the tag data against tampering by unauthorised entities. We focus on computational processes to ensure tamper-detection and binding, while mechanical approaches are discussed in deliverable 4.1.

In addition to general threats to supply chain security and threats aimed at bypassing security features, attacks can also be targeted directly at the technology used for product authentication. In case of an RFID system, these attacks include, e.g., blocking or deactivating tags, eavesdropping of radio communication, or jamming of RFID readers [BSI04b]. These attacks are specific to the technology employed and will therefore be addressed by task 3.3 – development of security concepts – for the selection of technologies that we consider appropriate for the PVI.

The remainder of this chapter is organised as follows: we start with a brief introduction to the concept of identity and identifiers, as establishing the identity of a product is a prerequisite for authentication. We then present five approaches to product authentication: direct authentication based on natural properties, authentication by checking a difficult to reproduce feature, checking the validity of unique identifiers, plausibility checks of track and trace data, and secure object authentication using cryptographically-enabled RFID tags. Next, we give an overview of the complementing concepts we have just motivated: copy protection of tags and tag data, methods for ensuring the binding between tag and product, protecting products against tampering, and performing status checks. We furthermore discuss potential problems typically associated with an RFID-based, online authentication infrastructure and show potential solutions. This concerns protecting the privacy of businesses and consumers as well as dependability issues of network based infrastructures such as security problems or performance bottlenecks. We also highlight the implications of combining various authentication approaches and features. We conclude this chapter by analysing the strengths and weaknesses of the described authentication approaches.

2.2 Identity and Identifiers

According to [Sta02], “authentication is the process of verifying a principal’s claimed identity. It is the logical step that follows identification, i.e. establishing who that principal claims to be.” It is therefore necessary, before presenting authentication methods in the following section, to briefly introduce the concept of identity. Moreover, with the advent of large-scale RFID deployments, methods for uniquely identifying objects and mass serialisation have become important topics. We will revisit three aspects of identity: the level of granularity at which *identity* can be established, ways of *coding and representing identity*, as well as *data carriers*, i.e. technologies for adding this codified identity to products.

2.2.1 Identity

Every single object has a unique identity that can be revealed, if only its properties are measured accurately enough. A convenient metaphor for identity is the soul of the

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

object. The identity of an object does not change during its lifecycle and is independent from any identifier associated with it; otherwise changing the identifier would also change the identity of the object. Instead of identifying each item uniquely, for practical reasons, identity is often established at a less granular level. Most conveniently, all objects belonging to a certain class are subsumed under a group identity, e.g., *a can of coke*. In contrast, objects can also be given a unique or individual identity, *the can of coke number 12345*. In between those two extreme points, one will find for example the batch identity, or the set of all pharmaceuticals produced by a certain production line in a certain factory. Therefore identity can be perceived as a continuum, ranging from object class to unique identity. To facilitate the identification of objects, their identity is often codified and attached to the product in form of an identifier.

2.2.2 Coding and Numbering schemes

The identity of an object can be codified and represented in a human and/or machine readable way. In general, the identity of an object is represented by an identifier, a lexical token that names entities. In practice, identity and identifier can in most cases be used synonymously and we distinguish between them explicitly when needed. A coding system describes how an identifier is constructed according to an agreed set of rules. The 13 digit International Book Number (ISBN) for example is an identifier for books, represented by a concatenation of natural numbers from zero to nine and hyphens according to certain rules. Unique identifiers are identifiers that are guaranteed to be unique among all identifiers used for a set of entities. Note that ISBNs are also regarded as unique although two copies (instances) of the same book (class) have the same ISBN as the definition of uniqueness depends on the definition of entities. In the context of RFID and product authentication, the term unique identifier mostly refers to identifiers that are unique for every single item, i.e. in a way that two different products of the same type have different identifiers (also called globally unique identifier). For the sake of simplicity, in this document, the term unique identifier will always refer to such an individually unique (instance) identifier. Assigning unique identifiers to individual products is also called mass serialisation.

A popular coding system is the global trade item number (GTIN) or EAN/UCC-14 format, an umbrella term used to describe an entire family of numbering schemes that are usually represented by barcodes. The GTIN is for example a superset of the ISBN-13 (a 13-digit ISBN), but more notably of the European Article number (EAN) and the universal product code (UPC) that are used for representing article numbers in Europe and the US respectively³. These codes do not differentiate between individual copies of the same product. The EAN (in clear text and represented by a barcode) can be found on almost every consumer product sold in Europe today. The numbering structure of a GTIN comprises an indicator digit for the packaging level at which the GTIN is assigned, a company prefix, a product reference number assigned by the company and a check digit [Bro01b].

There exist many industry-specific and country specific coding systems. One example is the National Drug Code (NDC) that is assigned to certain pharmaceuticals traded in the US. Like many coding schemes, the NDC is constructed hierarchically. The NDC is a 10-digit, 3-segment number, consisting of an identifier for the manufacturer (or

³ <http://www.gtin.info/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

distributor), a product code specifying the strength and dosage form, and a package code that identifies the size of the package. Another example of an industry specific scheme is the ATA Spec 2000 for the aerospace industry [HS06].

A numbering system especially designed for the combination with RFID is the Electronic Product Code (EPC) [Bro01a]. It was developed by the Auto-ID Center, a former industry funded research consortium at MIT. In 2003, MIT licensed the technology to the Uniform Code Council (today: GS1 US), which established a new subsidiary, called EPCglobal, to operate the EPC system all over the world. The labs were renamed Auto-ID Labs and funded by EPCglobal to continue advanced research related to the EPC System [SAB07].

The EPC numbering scheme (see Figure 3) consists of four distinct partitions: version number, domain manager number, class code, and serial number. The first partition, the version number, contains information on the length and structure of the code being used, and the three remaining partitions contain the actual unique identifier for the product [SAB07]. Therefore, the EPC is similar to a GTIN, augmented with a unique serial number for each product [Bro01b]. As the EPC combines the object class with a serial number, the EPC is not only a unique identifier, but a globally unique identifier, meaning that any two items do not have the same identifier, irrespective of the object class they belong to. Although designed with RFID in mind, there are no technical barriers for the usage in combination with other techniques [O’C05]. Another example of a globally unique identifier is the universal item identifier (UID) that the US department of defence mandates to be put on high value goods.

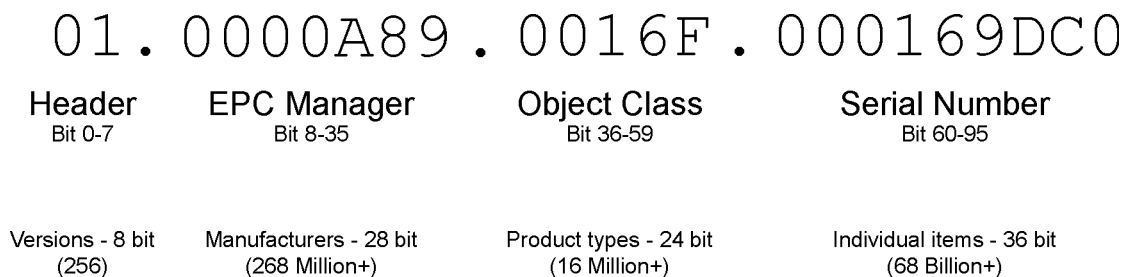


Figure 3: The Electronic Product Code

In addition to the coding systems used in the inter-organisational context, companies internally use proprietary numbering schemes. One example are stock keeping unit (SKU) numbers, which are similar to EAN-based article numbers, but there is no standard prescribing how to assign SKUs. Often, they are assigned at a more granular level than EANs, for example to differentiate between articles with varying colours. In fact, SKUs can be attached at any level that makes sense for the operations of a company, e.g., to items, product variants, product lines, bundles, services and the like. If goods identified by an SKU are to be exchanged with other companies, the SKUs usually have to be cross-referenced to standardised numbering schemes. In some industries, e.g., the luxury goods industry, high-value goods are serialised on item level using continuous numbers.

2.2.3 Data Carriers

The identifier needs to be attached to the product it names. A simple way is to print, engrave, emboss, or etch an alphanumeric code in the product. Another possibility for

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

symbolising the identifier is the barcode, a pattern of black and white lines which can be scanned quickly with an optical reader. The linear or one dimensional barcode is a pattern of bars and spaces that encodes a number according to a code table. Two dimensional barcodes like the Data Matrix code (see Figure 4) or the High Capacity Color Barcode⁴ are able to store more information than their one dimensional predecessors. Depending on the symbol size, a Data Matrix code can encode up to 3116 numbers or up to 2335 characters. A three dimensional barcode that can store even more data was developed by the National Physical Laboratory in the UK.⁵ It is based on nanotechnology, is invisible to the naked eye, and consists of a silicon cube measuring 30 microns across in which holes of varying depth are drilled to store the encoded information.

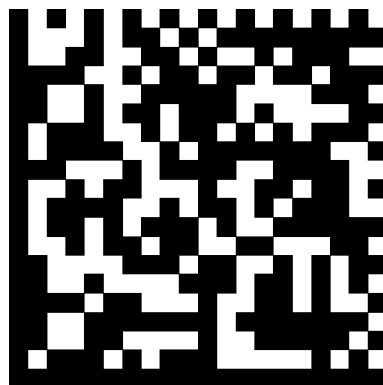


Figure 4: Data Matrix Code with a Symbol Size of 20x20

RFID tags are another data carrier that can be used for assigning a unique identifier to a product. RFID is a promising technology to be used in various application areas, including anti-counterfeiting. A small electronic device, a microcontroller with computational unit, memory, and a radio-frequency interface for wireless communication, is packaged as an RFID label or RFID tag that comprises the microcontroller itself, an antenna, and coating, which protects the microchip against damage. Such a tag can be applied directly to a product or its packaging, or can even be integrated during the manufacturing process. A *reader* device is then used to supply the tag with power, and to communicate with it, both wirelessly. The reader and the tag can exchange data, and they can both perform computations. However, the computational power of a tag is limited due to size and power constraints.

RFID supports most features that data carriers can provide, such as unique identifiers and contactless interrogation. These basic features can be implemented with low complexity on a microcontroller; therefore such tags can be quite inexpensive and are suitable for mass deployment. If the application case justifies it, more complex functionality can be implemented. Thereby, additional features can be offered, such as data storage and computational capabilities [Fin06]. One can distinguish between read-only (RO), write once/read many (WORM), and read/write (RW) tags. The computational capabilities can be used to implement additional security features, such as access control to specific memory areas, cryptographic protocols, or anonymity. Within the domain of RFID, a distinction is made between active and passive RFID

⁴ <http://research.microsoft.com/research/hccb/>

⁵ <http://www.npl.co.uk/review/2005/innovation.html>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

tags. While active tags have an onboard power supply, passive tags are powered by the interrogating reader. Active RFID tags can provide enhanced security features, but in turn they are more costly and bigger in size. This limits their use in many scenarios.

In addition to EPCs, tags can store other identifiers or even multiple identifiers at a time. They may also store additional object information like an expiry date or the manufacturing time of a product. The advantage of RFID compared to barcodes and alphanumeric printing is that many tags can be read simultaneously (bulk reading), without line of sight and regardless of the orientation of the products.

Clear text, barcodes, and RFID are the most common carriers of identifiers, but there are many more possibilities. Unique identifiers may also be represented by chemical or physical markers called taggants (the word originates from the trademark *Microtaggant*), for example by microscopic particles consisting of several coloured layers⁶. Depending on the manufacturer, these taggants allow millions or even billions of different colour codes. By combining numerous particles the number of codes is practically infinite. Taggants can be integrated into many types of material like plastic resins, films, adhesives, printing inks, and papers.

2.3 Product Authentication

Product authentication means verifying a product's claimed identity and thereby proving that the product is genuine [GC06]. In the previous section we explained how objects can be identified and we will now focus on how the claimed identity can be verified. Traditionally, in security related publications, it is suggested to check *something an object knows, something an object has, or something an object is* in order to authenticate it. These checks can also be applied to people, typical examples being passwords, passports and iris scans. These checks may be combined to multifactor authentication so as to obtain higher security levels. However, this classification is not exhaustive: authentication might also be based on *something an object does, where an object is*, or further methods that imaginative people come up with [Sta02].

These authentication methods can be applied for deciding whether a product is genuine or not. First of all, the decision can either be based on *something the product is*, i.e. an innate property of the product, or on *something the product has*, i.e. on the properties of an artificial feature that is added to the product. In the latter case, as we already stated, ensuring a proper binding between the product and the artificial feature is essential. The harder it is to reproduce the artificial feature, the more reliable the authentication will be. Hard to reproduce features range from features that are impossible to clone, difficult or time consuming to copy, to features that are financially infeasible to clone. On the other hand, even the mandatory presence of – by default cloneable – RFID tags on certain objects will help to identify objects not bearing a tag as counterfeits. The cost and effort for getting RFID tags, storing valid identity numbers on them, and attaching them to counterfeit products might initially suffice to put off counterfeiters.

An important property that can be added to a security feature is a unique identifier. The presence of a unique identifier or respectively its carrier (e.g., an RFID tag) is the first step in authenticating a product, but the introduction of unique identifiers enables

⁶ <http://www.secutag.com/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

much more sophisticated decisions algorithms. The number can be checked for validity or used as a pointer to additional information about the product, its history, the transactions and events it was involved in, and the locations that the product visited. Thus, the product can be authenticated based on *what it did and/or where it was*. If the feature added to a product is capable of storing data or performing cryptographic operations, the authentication can be based on *something the product knows*.

The following sections contain a more detailed description of these five authentication methods. Table 1 summarises the title of each section, the authentication approach described therein, and the type of question that is asked to decide whether a product is genuine. Furthermore, technologies that may be used for realising each approach are listed as examples. By definition, authentication approaches are technology agnostic as they focus on how a decision is taken. But not all methods can be combined with all potential technologies and some technologies cannot be used for certain approaches or are suitable for multiple approaches at a time. For example, RFID tags can be checked for presence, whether they store a valid serial number, whether the product history associated with that number is plausible, and whether they know a certain secret, thus allowing for a reliable multifactor authentication.

Section Title	Approach	Decision Criteria	Technologies
2.3.1 Direct Authentication	Something the product is	Do the innate properties of a product match with those of a genuine product?	(Forensic) physical, chemical or optical analysis
2.3.2 Authentication Based on Difficult to Reproduce Features	Something the product has	Is an artificial (hard to reproduce) security feature present?	E.g. watermarks, invisible inks, copy detection patterns, 2D-barcodes, RFID tags, etc.
2.3.3 Verification of Unique Identifiers	Something the product has	Was an item with the identity the product claims to have actually produced?	Any technology suited for mass serialisation, e.g. 2D barcode, RFID, printed numbers, etc.
2.3.4 Plausibility Checks of Track and Trace Data	Something the product did	Is the history that an object claims to have plausible?	Any technology suited for mass serialisation, e.g. 2D barcode, RFID, printed numbers, etc.
2.3.5 Secure Object Authentication	Something the product knows	Does the product know a secret that only a genuine product would know?	RFID

Table 1: Approaches to Product Authentication

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

All authentication approaches require some reference data that is compared to the features or other credentials of the product. In general, the reference data tells what the genuine product should be like, should have, should know, or where it should be. For some authentication approaches, the use of an IT system and a database storing reference data is mandatory (sometimes referred to as *online* approaches); others will work both with and without such a system (*offline* approaches). IT systems play a central role for checking the validity of unique identifiers as well as for verifying whether a product knows a secret key. For direct authentication and authentication based on an artificial feature, some technologies will rely on a database with reference data while others are self-contained and operate stand-alone. The check of a watermark on a banknote is an example of such a stand-alone, offline check. In that case, the reference data is the knowledge that an original banknote must have a certain watermark. Direct authentication and authentication based on a hard to reproduce feature have in common that the security is based on the manufacturing process of the product or the tag. For the other three authentication approaches, security is established by a computational process (alone). In this report, we will therefore focus on the verification of unique identifiers, plausibility checks of track and trace data and secure object authentication. We will also give a brief overview of direct authentication and authentication based on hard to reproduce features, but these approaches will be covered in detail by deliverable 4.1. This distribution is illustrated in Figure 5.

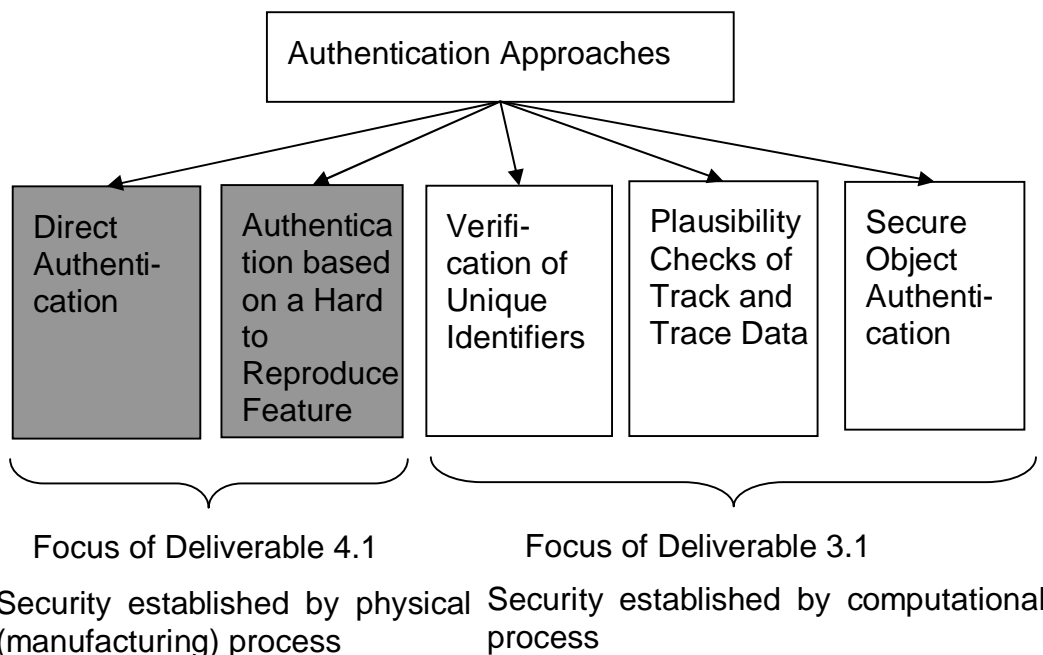


Figure 5: Distribution of Description of Authentication Approaches

2.3.1 Direct Authentication

Direct authentication is based on something a product is, i.e. on a product inherent feature. The exploitation of a natural product property distinguishes direct authentication from all other authentication approaches described, as they are based on an artificial feature that is added to a product with the purpose of enabling authentication. As no tagging or labelling is necessary for direct authentication, these

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

approaches will not generate tag and tag application costs and no measures for ensuring the binding between the tag and the product have to be taken.

First, one has to choose the property or the set of properties that direct authentication should be based on. Ideally, the property (or the combination of properties) should be

- unique to every single item,
- inimitable, i.e. should not be cloneable or easy to reengineer,
- and stable, i.e. should not change during the lifecycle of a product.

Not all properties chosen will satisfy all of these conditions. The properties might not be unique on item level, but on class level or for a certain set of objects. These properties can nevertheless be used for direct authentication, but the security level will not be as high as with uniquely identifying properties. Similarly, the easier it is to reproduce a product property, the more the security level will decline. Properties might change slightly during the lifecycle of a product, e.g., by deteriorating or corroding, but they must maintain a certain level of stability to be usable for direct authentication.

The product properties that can be measured for authentication purposes are very diverse and include

- physical properties, e.g., weight, density, etc.,
- chemical properties, e.g., ingredients, composition, etc.,
- visual properties, either the general appearance of a product or on microscopic level, e.g., the surface structure of a product, etc.

In order to authenticate a product, the selected properties must be measured and compared to the properties of a genuine product. Again, there are different ways to perform the comparison. One can compare the properties of the product in question with those of a genuine reference product. The properties of a product can also be recorded in a database and retrieved for comparison. If the properties are more complex, they are often transformed into a so called product fingerprint before being stored. This fingerprint may be attached (e.g. printed) to a product and/or stored in a database. Comparing a suspected counterfeit to the attached fingerprint of its own properties without double-checking this information with data from an objective source, e.g., the brand owner's database, will not enable to authenticate a product. Lastly, if neither a reference product is available nor product properties were recorded, a human expert might be able to judge whether a product is genuine or not by comparing the product properties with his knowledge about original products. The different possibilities are summarised in Figure 6.

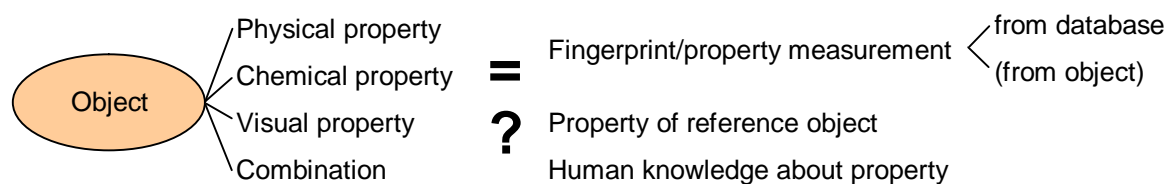


Figure 6: Direct Authentication

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Technologies suited for direct authentication are described in deliverable 4.1. All of these methods will benefit from a reference property or product fingerprint that is stored in a database for later comparison.

In short, relevant technologies for direct authentication comprise:

- Image Comparison: The manual or automated comparison of specific product features with a photo of an original product.
- Surface analysis: A fingerprint of a laser scan of the surface structure of a product is captured at manufacturing time and stored in a database. The fingerprint is unique to a single product.
- Forensic analysis of chemical and physical product characteristics, such as weight, colour, and chemical composition.

2.3.2 Authentication Based on Difficult to Reproduce Features

This authentication approach is based on something the product has, i.e. on an artificial feature that is in or on the product, and on the authenticity of that feature. First, it needs to be checked whether the feature is actually present, and in the next step, whether the feature is authentic. The harder it is to reproduce the selected feature, the more secure the authentication becomes. This means that not every tagging technology is suited for reliably detecting counterfeits. The difficulty in reproducing a feature might have different reasons, among them are

- the costs for reproducing the feature or for attaching it to a product,
- no access to the material needed for imitating the feature,
- no access to the production facilities needed (e.g., for manufacturing RFID tags),
- no knowledge about the (complex) production process or the materials needed,
- no knowledge about the presence of a feature (covert and forensic features),
- intrinsically not reproducible features, i.e. features that can be produced and verified, but not reproduced voluntarily,
- and features that contain cryptographically protected data (see section 2.3.3),

Authenticating a product by relying on a copy protected feature is in many ways similar to direct authentication, except for the nature of the property that the authentication is based on. As an artificial feature is authenticated instead of the product itself, it must be ensured that the feature is not separated from the product (see section 2.5). Like the natural properties of products, added features have different properties, i.e. they can be divided into optical, digital, physical, and (bio-)chemical features. Some of the features can be augmented with data, which offers additional possibilities for authenticating products.

Moreover, one can distinguish between overt, covert, and forensic features. While overt features are visible to the human eye and can usually also be checked by consumers, covert features are hard to detect, often require special equipment for verification, and their existence is not publicly disclosed. Forensic features are not visible and can only be checked with special equipment. As with product intrinsic properties, artificial features can be unique on item, batch, or object class level. As

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

with product intrinsic properties, reference values can be stored in a database, added to a data carrier on the product, or the authenticity of features can be judged by an expert.

Artificial security features are described in detail in deliverable 4.1, which presents the state-of-the-art in smart tagging technologies. In this report, we will give a short summary of the technologies described in deliverable 4.1:

Optical overt:

- Security inclusions, comprising security paper, and watermarks embedded in paper
- Security printing, including lithographic and intaglio printing, printed security images (e.g. guilloches), and security backgrounds
- Security inks, including photochromic (light reactive) and thermochromic (heat reactive) inks
- Diffractive optical devices (DOVID), including two and three dimensional holograms

Optical covert:

- Microscopic particles, e.g., microtaggants
- Microprinting and labels
- Spectroscopic techniques, requiring taggants that can be detected when exposed to various light energy sources or chemical reagents

Digital covert

- Digital watermarks, which are encrypted texts or images (e.g. a serial number) that are hidden in the noise of digital images that are printed on products or packages [PAK99].
- Copy detection patterns (CDP): they are based on the fundamental principle that any optical replication technology will result in an information loss compared to the original image. The CDP is a noise pattern that is printed on a product and at the same time stored in a database. For verification, the CDP is scanned or photographed and compared to the original. If the correlation between the two images is above a certain threshold, the product is genuine. It is also possible to store only the seed needed for generating the CDP and to recreate the reference image on the fly. Additional data, e.g. an identifier, can be embedded in the CDP. The creation and verification of CDPs may be secured with cryptographic keys.

Covert Forensic

- Taggants, which are chemical or biological markers added to a product or its packaging, including low concentrations of marker chemicals that can be detected with spectrometry, fluorescence, or other chemical analysis methods and DNA markers.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- Component analysis, including colorimetry, chromatography, measuring of density, solubility, viscosity and refractive index. These methods can also be used to test the properties of artificial features and markers added to products.

2.3.3 Verification of Unique Identifiers

2.3.3.1 General Approach

Assigning unique identifiers to individual products provides a cost-effective countermeasure against counterfeit trade and grey market activities. Unique identifiers can be used to detect counterfeit products as well as to detect grey market activities by verifying identifiers and analysing the supply chain. This can be done by choosing a numbering technique that is difficult to apply for illicit actors, but easy to check for supply chain partners or end users ([Joh05], [SMTF06]).

According to [SMTF06], an ideal scenario would look like this:

- The unique identifier is assigned in a random way, with the numbering space significantly larger than the number of products to be identified, so that illicit actors cannot simply guess valid identifiers.
- The validity of the unique identifier can be easily checked by the supply chain partner or, if desired, by the consumer.
- The unique identifier can be read automatically by authorised persons, allowing for large scale searches for invalid or duplicate identifiers, thus increasing the chance to seize illicit goods.
- A duplication of the carrier of the unique identifier is not possible or is unreasonably expensive.
- The carrier of the unique identifier cannot be removed nor can illicit actors overwrite the identifier to disguise the identity of the object.

A simple distributed architecture of a system that enables the verification of unique identifiers is shown in Figure 7.

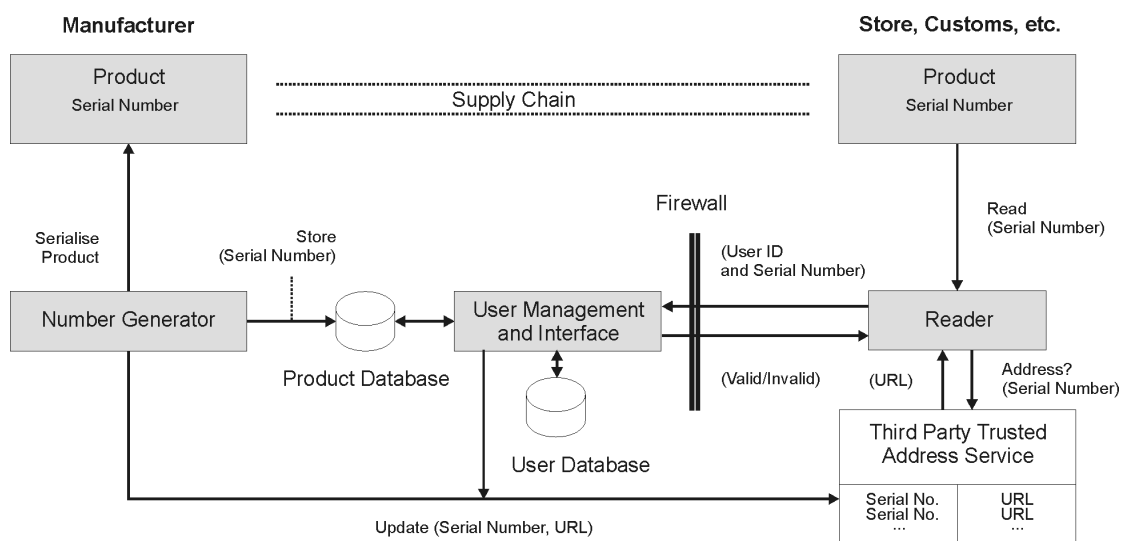


Figure 7: Architecture of a System for Verifying Unique Identifiers

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

In this architecture, unique identifiers are assigned to products. To minimise the possibility of successful number guessing, unique identifiers should have a considerable length and be randomly generated.

Valid unique identifiers are stored in a database of the manufacturer or of a trusted third party. Dedicated verification servers protected by access control mechanisms are connected to these databases and the internet. When a trusted supply chain partner wants to verify a unique identifier, the partner first has to find out the respective verification server. This could be realised by a lookup service comparable to the Domain Name Service (DNS) that links unique identifiers to verification servers.

2.3.3.2 Verification of Unique Identifiers based on RFID

The architecture described in the previous section is perfectly suited in a scenario where products are equipped with RFID tags. The identifier does not have to be carried on an RFID tag as other data carriers like 2D barcodes are also an option. However, the speed and convenience of the checking process will depend on the type of data carrier used. The advantages and disadvantages of different types of data carriers have been addressed in section 2.2. In case of RFID, serial numbers, e.g., EPCs (see section 2.2), are written to tags and the product database of the manufacturer. RFID tags are also suited to store very large numbers to avoid number guessing.

As described in section 0, not all RFID tags are read-only. Illicit actors could read serial numbers from licit products and write these numbers to plain WORM or RW tags that are later attached to illicit products thus compromising the security system.

However, there is a possibility to significantly improve security of simple RFID tags (e.g., most Generation 2 EPC tags) as they have a read-only field containing a transponder ID number (TID) similar to the unique media access control address of network interface cards. In addition to the unique identifier of a product, the content of this field can be stored in the database and used to verify the identity of the tag and thus of the product.

To copy the TID and the unique serial number of an authentic RFID tag, illicit actors would have to be able to manufacture their own RFID tags or to use fully programmable tags, presenting an additional cost factor or a barrier for illicit actors.

2.3.4 Plausibility Checks of Track and Trace Data

Unique identifiers not only can be directly used for authentication as described in section 2.3.3. Trace data of unique identifiers that originates from readings at different partners within the supply chain can also be used in certain scenarios to detect suspicious movements of products. In addition, trace data is the foundation for electronic pedigrees. Again, there are several options for choosing the data carrier that creates the foundation for track and trace and also has a strong influence on the overall performance of a track and trace system.

As an example, the following sections describe how trace data in the context of RFID can be used for authentication. With RFID, trace data can be stored on the tag directly or on the network. In some cases, both methods can be included in an integrated approach [DMS07]. The section about data-on-network puts special emphasis on the standardised EPCglobal Architecture Framework.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

2.3.4.1 Data-on-Tag

Data-on-tag means attaching products with RFID tags that store a unique identifier and additional data. Compared to the centralised data-on-network approach, data-on-tag aims at decentralised data management.

Storing data directly on tags makes sense if it is crucial to read or write this data even if there is no network connection. This way, product and process information can be changed dynamically and automatically along the supply chain, which ensures a parallel flow of material and information [Hom05]. The data-on-tag approach is also preferable if decisions have to be made or data has to be recorded in real time. Another argument for storing data on tags directly is if the frequency of data access is so high that the cost of data transmission is greater than the cost of writable tags [MP05]. Expiration data, hazardous goods information, history data, manufacturing recipe, permissible configuration, or quality grading are examples of possible records that could be stored on tags.

Storing trace data or even electronic pedigrees on tags themselves does not seem feasible as passive RFID tags nowadays have only up to 8 KiB of memory [Fin06]. Encrypting or signing this data is even worse as an RSA signature alone requires 1 KiB of memory. More powerful RFID tags might allow storing trace data on tags in the future that could be used for authentication.

2.3.4.2 Data-on-Network

Data-on-network means attaching products with RFID tags that only store a unique identifier and no additional data. This identifier then acts as a pointer to further information about the product that is stored in company-internal databases.

Data-on-network itself comes in two flavours: centralised and decentralised. In the centralised approach all information about products is stored in a single database. This makes sense if data capture and access are performed within a single organisation. In case of sensitive data where the access to a database needs to be strictly controlled, centralised data management might be the only acceptable solution. An example for the centralised approach is the Bollino system that is used for drug tracking in Italy. In most cases yet it is more practical to distribute data among multiple databases each owned by a different supply chain partner. This approach reflects the distributed nature of supply chains much better.

Storing data within databases on the network has the advantage that data is available even if the object is not. Another benefit is that low-cost tags are sufficient for this approach as only an EPC number has to be stored. Compared to the data-on-tag approach storing data on the network also might be preferable as there is already a well accepted standard available, which is discussed in the following section. Dependability issues such as performance, availability and security of network based approaches will be discussed further in section 2.9.

2.3.4.2.1 EPCglobal

An architecture that is based on the data-on-network paradigm is the one proposed by EPCglobal. The EPCglobal Architecture Framework is a collection of interrelated standards for hardware, software, and data interfaces, together with core services that are operated by EPCglobal and its delegates, all in service of a common goal of enhancing the supply chain through the use of EPCs [EPC05c].

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

The EPCglobal Architecture Framework specifies interfaces of five EPCglobal root services: Subscriber Authentication, Discovery Services (DS), Object Naming Service (ONS) Root, Manager Number Assignment, and Tag Data Translation Schema. The first three of these are network services while the last two are offline, business services. These services are introduced below:

- Subscriber Authentication enables any EPCglobal Subscriber (any organisation that uses EPCglobal core services) to authenticate the identity of any other EPCglobal Subscriber without prior arrangement between the two parties. This service is not specified yet, but EPCglobal has specified an EPCglobal certificate profile that defines how different entities in the EPC network are authenticated using public-key infrastructure [EPC06g].
- Discovery Services (previous term: EPCIS Discovery) may be used by an EPCIS accessing application to locate the EPCIS services of all EPCglobal Subscribers that have information about the object in question, including EPCglobal Subscribers other than the EPC Manager (an EPCglobal Subscriber who has been granted rights to use a portion of the EPC namespace by an Issuing Agency) of the object. The EPC Information Services (EPCIS) is explained in the following section. This service is not specified yet, but once available, it will make ONS (below) obsolete by providing the same functionality (and more).
- ONS Root [EPC05d] can be thought of as a simple lookup service that takes an EPC as input, and produces as output the address (in the form of a Uniform Resource Locator) of the desired service associated with the EPC, e.g., an EPCIS service. In most cases ONS Root would delegate the request to the Local ONS service of the EPC Manager organisation for that EPC. This hierarchical approach ensures scalability and eases maintenance of the lookup database.
- Manager Number Assignment ensures global uniqueness of EPCs by maintaining uniqueness of EPC Manager Numbers assigned to EPCglobal Subscribers and assigns new EPC Manager Numbers as required by EPCglobal Subscribers.
- Tag Data Translation Schema provides a machine-readable file that defines how to translate between EPC encodings defined by the EPC Tag Data Specification [EPC06d].

There are three groups of standards within the EPCglobal Architecture Framework:

- EPC physical object exchange standards describe protocols that define the physical and logical requirements for passive-backscatter RFID systems. The categorisation of these protocols is based on the different frequency ranges and the underlying tag classes, e.g., there is a Generation-2 UHF protocol for Class-1 tags [EPC05b]. The object exchange standards also contain EPC tag data standards that define completely that portion of EPC tag data that is standardised, including how that data is encoded on the EPC tag itself (i.e. the EPC Tag Encodings), as well as how it is encoded for use in the information systems layers of the EPC Systems Network (i.e. the EPC URI or Uniform Resource Identifier Encodings) [EPC06c].

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- EPC infrastructure standards define interface standards for the major infrastructure components required to gather and record EPC data. Contained are standards that define the protocol by which tag readers interact with EPCglobal compliant software applications [EPC06f] and the protocol used by management software to monitor the operating status and health of EPCglobal compliant RFID Readers [EPC06e], a standard for the conversion between different representations of an EPC [EPC06d], an interface specification through which clients may obtain filtered, consolidated EPC data from a variety of sources [EPC05a], and the specification for the EPCIS Capture Interface that defines the delivery of EPCIS events from EPCIS Capturing Applications to other roles that consume the data in real time [EPC06a].
- EPC Data Exchange Standards provide means to share data about EPCs between supply chain partners through peer-to-peer interaction and also provide access to EPCglobal core services and other shared services that facilitate these exchanges. Contained are interface specifications by which EPCIS data can be retrieved by an EPCIS Accessing Application [EPC06a] as well as the three core services ONS, DS, and Subscriber Authentication.

The EPCglobal network architecture is shown in Figure 8.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

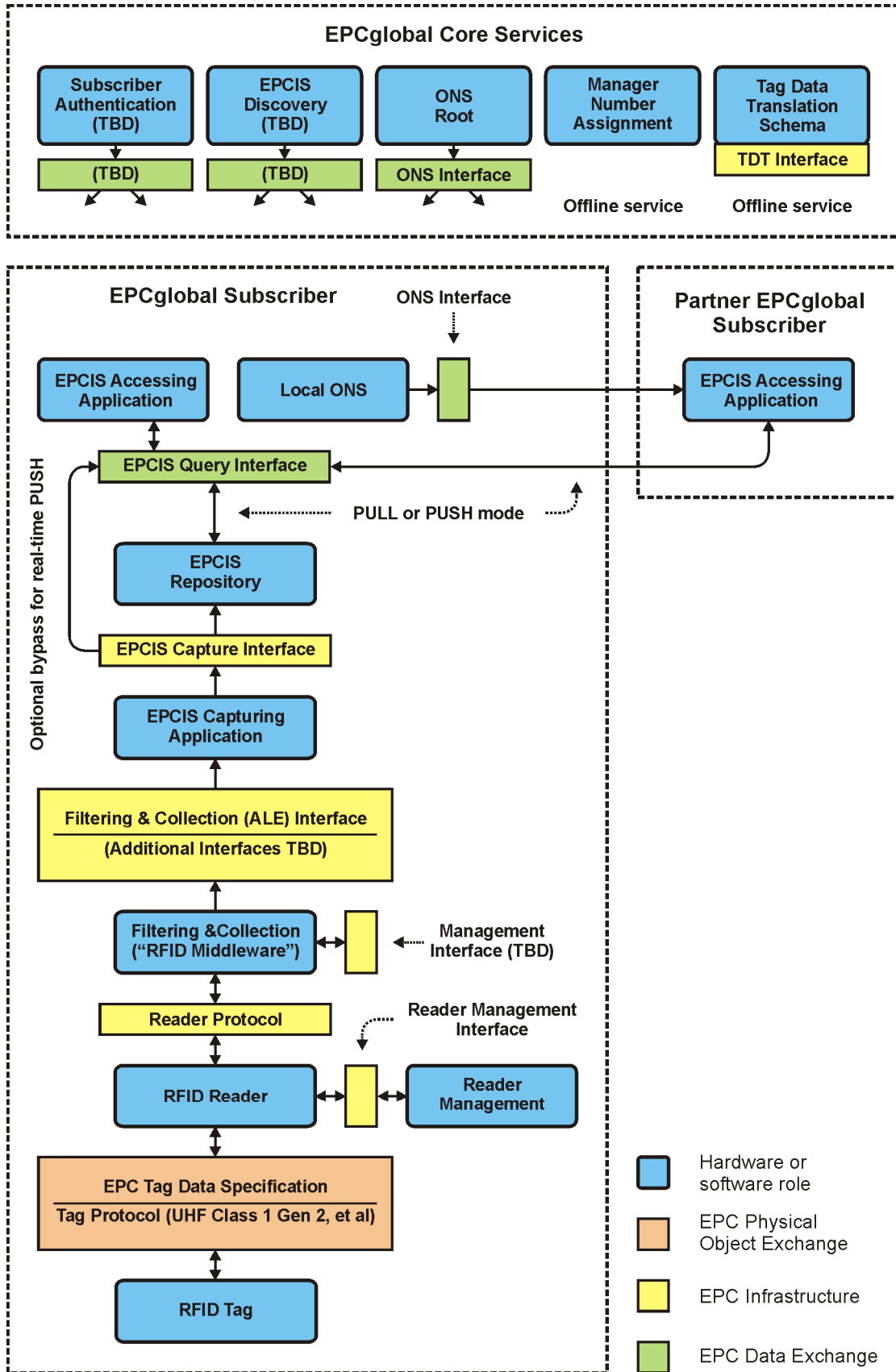


Figure 8: The EPCglobal Network Architecture

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

2.3.4.2.2 EPC Information Service (EPCIS)

One of the main ideas behind the EPCglobal architecture is to label individual products with unique EPCs.

While these products move through the supply chain, certain events can be generated. The most common event is that a product has been spotted, i.e., an RFID reader has read the EPC stored on an RFID tag that is attached to the product. An event can also be generated if a product enters or leaves the supply chain, i.e., if it is issued by the manufacturer or sold to a customer. During the lifetime of a product it could also be associated with other products, e.g., a product could be packaged together (aggregation) with other products of the same kind whereas the package containing the products is labelled with an EPC itself. At a later point in time, this association could be broken up again (disaggregation), for example because the products are repackaged. Further examples are quantity or transaction events. Quantity events describe a sighting of a set of identical products, without specifying single EPCs. Transaction events express the association or disassociation of products to and from business transactions, respectively.

These events are read at different points within the supply chain by the respective partner that stores the events in its local databases. Hence, information about a product that is moving through the supply chain is distributed within the network. Without common standards, sharing this data is a complex task.

The goal of the EPCIS [EPC06a] is to enable disparate applications to share EPC-related data, both within and across enterprises. Ultimately, this sharing is aimed at enabling participants in the EPCglobal Network to gain a shared view of the disposition of EPC-bearing objects within a relevant business context. The EPCIS specification provides XML schemata for describing the above mentioned events and interface definitions for capturing and querying them.

As the information about products is distributed within different databases, there has to be a mechanism that allows for finding EPCIS servers that have collected information about a given EPC. This component within the EPCglobal Network Architecture is the DS, but this component has not yet been specified. There are several possibilities how to design this service, ranging from a totally decentralised approach to a centralised one. The BRIDGE project⁷ is currently investigating which method meets industry demands.

Figure 9 shows an example supply chain consisting of four partners: a manufacturer of a product, a distribution centre, a wholesaler, and a store. Each partner maintains its own EPCIS. In addition, the manufacturer (EPC Manager) also possesses a local ONS that directly links to its EPCIS. When a product is moving from the beginning to the end of the supply chain (1, 2), partners store event data associated with the EPC of the product. If direct access to the EPCIS of the manufacturer is desired, the local ONS of the manufacturer would have to be retrieved first by performing an ONS Root lookup (3). The local ONS can then be used to access all services operated by the manufacturer, including the EPCIS. If all captured events that are associated with a specific EPC shall be retrieved from the network, the DS (no matter how it will actually be specified) can be used to return all relevant EPCIS (4) that can be queried consecutively for these events.

⁷ <http://www.bridge-project.eu/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

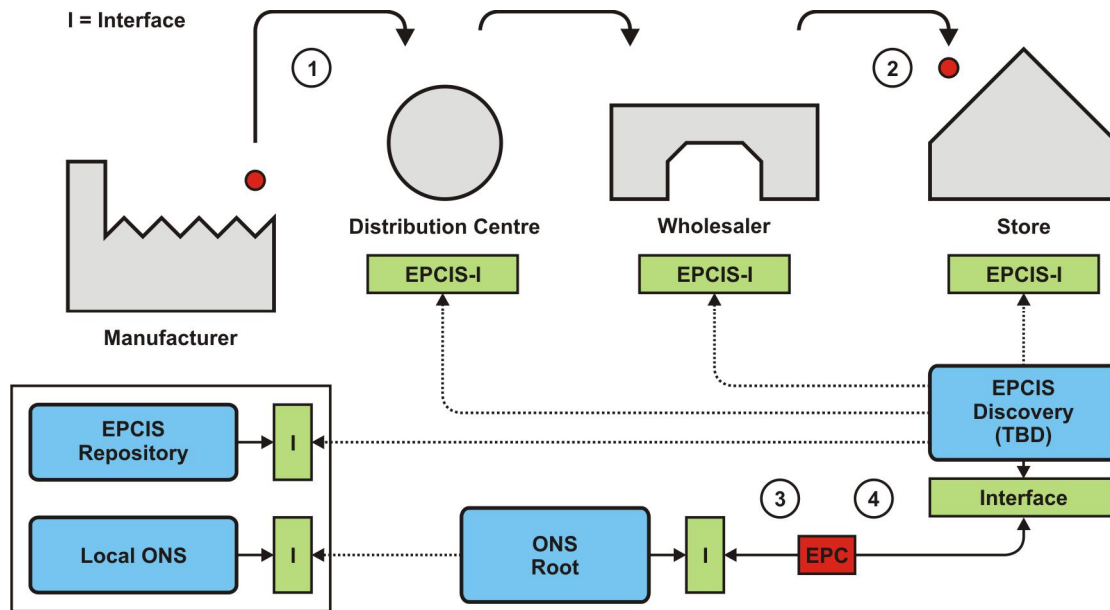


Figure 9: EPCIS and DS

As the EPCglobal architecture currently lacks three important pieces to enable cross-company traceability queries, the DS in particular, IBM Research has developed a software layer on top of EPCIS to efficiently navigate the EPCglobal network. The query middleware called Theseos provides traceability applications with the ability to execute complex traceability queries that may span multiple databases ([BGKR06], [IBM07], [CKS07]).

2.3.4.2.3 EPCIS and Plausibility Checks

Track and trace data, i.e. EPCIS events, can be used to authenticate products. Although not as reliable as secure object authentication [STF05] this approach is an alternative that does not require expensive RFID tags with cryptographic functions. If applied in combination with secure object authentication, it can also improve the overall reliability of a product authentication system.

A simple authentication check is to test whether a product arriving at a distribution centre is already marked as sold in the network. Plausibility checks can also test whether a product only showed up at allowed points (locations/companies) in the supply chain. If a counterfeiter duplicates RFID tags with a valid EPC, plausibility checks can be employed to test whether each EPC exists only once in the supply chain. Static rules can be applied to track and trace data to discover any discrepancies that point to the existence of suspicious products. Not much research has been conducted in this area. The SToP project will investigate this issue in more detail.

2.3.4.2.4 Electronic Pedigree

The term electronic pedigree, although in most cases used in the context of pharmaceuticals, in general represents the complete history of the chain of custody of a product in electronic form.

A simple electronic pedigree for example could contain the business name and address of each supply chain partner through whose ownership the product passed as well as the unique identifiers of the products that are associated with the pedigree. To protect such an electronic pedigree from manipulations, each partner has to have a

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

valid digital certificate to sign the updated pedigree with its digital signature. These pedigrees are usually transmitted in advance to the next partner within the supply chain. When the shipped products arrive at their destination, their unique identifiers are compared to the ones in the verified electronic pedigrees and thus authenticated. This technique is well suited for use with RFID tags as the authentication process can be automated to a large degree.

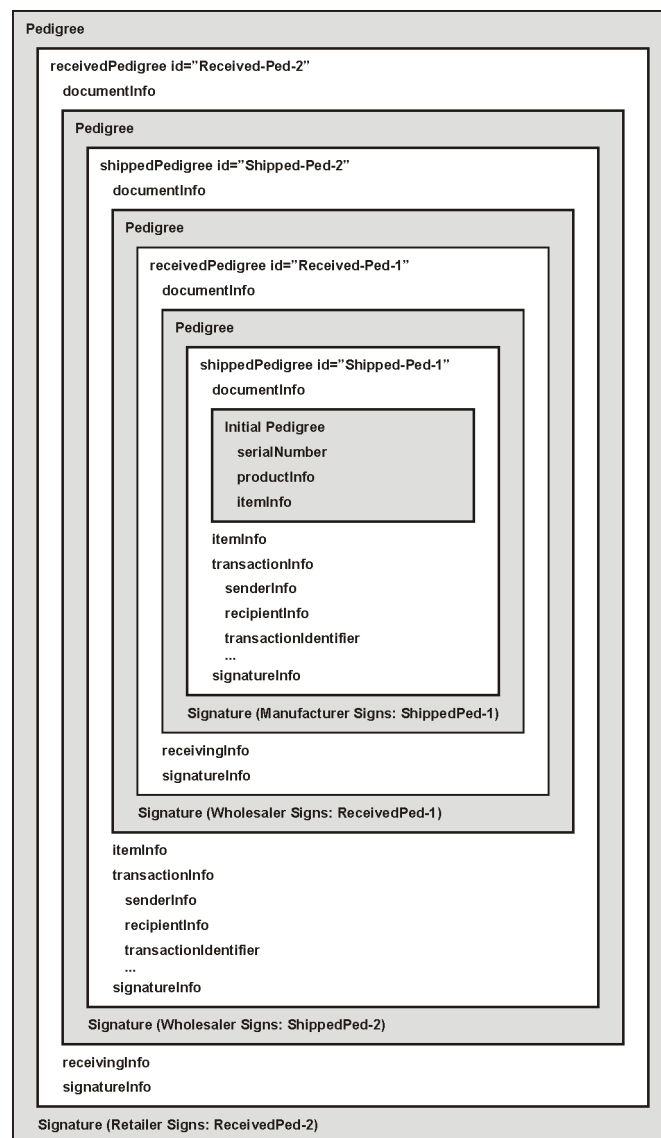


Figure 10: An Electronic Pedigree

Pedigrees are an important topic for the pharmaceutical industry, especially in the USA where federal law requires drug pedigrees since December 2006. A drug pedigree is a statement of origin that identifies each prior sale, purchase, or trade of a drug, including the date of those transactions and the names and addresses of all parties involved in them. In addition, a majority of states have more stringent pedigree requirements than those stated in the Prescription Drug Marketing Act (PDMA) and its amendments⁸. These pedigree regulations do not demand electronic pedigrees,

⁸ <http://www.fda.gov/cder/regulatory/PDMA/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

although there are many advantages in comparison to paper-based pedigrees. To ensure interoperability when exchanging electronic pedigrees, EPCglobal has recently released Version 1.0 of the Pedigree Standard [EPC07].

Important to notice is that legislation in some states includes item level product tracking while for example Florida requires only electronic shipping notice verification. Thus, there are two important definitions of electronic pedigree today. The first type, a serialised RFID approach, gives each product its own specific number which can be automatically captured as the product moves from one point in the supply chain to the next. The second, a simple file management approach, does not require product serialisation [Pea06].

Huang et al. [HVRZ07] claim that the EPCglobal network is not suited for creating electronic pedigrees as its central architecture might lead to scalability and privacy problems. Therefore, they propose an architecture that makes the creation of electronic pedigrees more robust, scalable, and secure by replacing the central ONS with a distributed lookup service that is based on distributed hash tables.

2.3.4.3 Hybrid Approaches

A solution for securing the pharmaceutical supply chain with RFID and public key infrastructure technologies that combines both the data-on-network as well as the data-on-tag approach was developed by Texas Instruments and VeriSign [Pea05].

Their solution called Authenticated RFID is based on special RFID tags with read-only unique identifiers for both the item and the manufacturer. The tags also contain a read-only digital signature that can only be verified by authenticated readers as well as a writable memory section. When a product is moving through the supply chain, event information is generated and stored in the network. The Authenticated RFID reader may also have the capability to digitally sign this event information to further increase security.

In addition, Authenticated RFID readers have the capability to write additional timestamps to the tag themselves. This timestamp provides an inseparable link and lookup index between the supply chain event, tag, and the corresponding external information.

2.3.5 Secure Object Authentication

2.3.5.1 Cryptographic Tag Authentication

The purpose of a cryptographic tag is the authentication of the tag itself, i.e. the verifying party should get a strong proof of the tag's identity. From a cryptographic point of view, this is possible by employing an authentication protocol. According to [MOV96], there are two basic possibilities for such protocols: (1) Password-based protocols and (2) Challenge-response protocols.

Password-based authentication protocols consider an identification process successful if a correct password is presented. A password can be any numeric value or a character string. It can be either universal or associated with a certain identity. It can be either fixed or dynamic. Usually, passwords are fixed values that are being used for every round of identification in the same way. Since they depend on static knowledge only, which can be easily transferred between (or stolen from) different entities, they provide only weak authentication.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Strong authentication is achieved through a dynamic mechanism that verifies that the entity that is to be identified is in fact actively participating in the protocol. Such a protocol involves at least the following two steps:

1. $A \rightarrow B : c$
2. $B \rightarrow A : f(c)$

Here, A is in the role of the verifier and B in the role of the prover. Entity A creates a challenge c and sends it to B. The challenge is freshly created for every execution instance of the protocol to make the use of old response messages useless. B applies a function f to the challenge and sends the result back to A. Function f can be based on a symmetric-key cryptographic encryption operation, a keyed hash function, or a signature algorithm. It is assumed that f can only be executed by A, since it involves a piece of secret information that is either only known to A (a secret key) or only known to A and B (a shared secret key).

A conventional symmetric-key authentication protocol can be formalised as follows:

1. $B \rightarrow A : \text{"I am B"}$
2. $A \rightarrow B : c$
3. $B \rightarrow A : f_{A-B}(c)$
4. A (verification): $g_{A-B}(f_{A-B}(c)) = c$

Here f_{A-B} denotes encryption with the symmetric secret key shared by A and B, and g_{A-B} denotes decryption with the same key. An asymmetric-key authentication protocol differs in so far as the verifier A decrypts the response. When f_B denotes encrypting with the secret key of B, and f_B^+ decryption with the public key of B, the conventional asymmetric-key authentication protocol can be formalised as:

1. $B \rightarrow A : \text{"I am B"}$
2. $A \rightarrow B : c$
3. $B \rightarrow A : f_B(c)$
4. A (verification): $f_B^+(f_B(c)) = c$

In principle, conventional authentication protocols can be applied in the RFID domain, and there are commercial products available that offer the required capabilities, such as symmetric encryption algorithms. These products are similar to smart cards with respect to their functionality and their application domains. Usually, they would be too costly for item-level tagging except for high-valued goods. Examples of such products which support cryptographic algorithms like DES (symmetric-key encryption) or others are NXP's MIFARE family of smart card controllers⁹, Infineon's SLE55Rxx¹⁰, or ATMEL's e5561 [ATM06].

Two reasons, however, are prohibiting the use of conventional cryptographic protocols in many cases. First, the constrained resources of RFID tags do not allow the use of cryptographic primitives in many cases due to performance and cost constraints. Making cryptographic primitives available for RFID tags is one research

⁹ <http://www.nxp.com/products/identification/mifare/>

¹⁰ <http://www.infineon.com/cgi-bin/ifx/portal/ep/channelView.do?channelId=-64715&pageTypeId=17099>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

track that is currently being pursued. Second, usually an identification step is required before authentication can take place. This allows the verifying party to select the appropriate key. However, *promiscuous* identification is contrary to privacy concerns that often go along with RFID technology. Thus, one of the major research goals in RFID security is *private authentication*. This problem has been stated as follows [MW04]: “how can two parties that share a secret authenticate each other without revealing their identities to an adversary?”

Moreover, the secret keys embedded in an RFID tag need proper protection against reading. Protecting keys is a hard problem as previous research in the area of smart cards has shown [AK96]. Due to the low cost of RFID tags, it is likely that they will not have as strong protection mechanisms as smart cards. On the other hand, the effort an attacker will be willing to invest in re-engineering the keys will be much lower for RFID tags. It is likely that the requirements will evolve over time as soon as real-world attacks surface. This also shows that relying on one security feature alone makes a system vulnerable.

We are now going to discuss the major approaches to RFID tag authentication, distinguishing between lightweight (non-cryptographic) approaches to secure object authentication and approaches based on strong cryptography for RFID tags. Other surveys relating to RFID security can be found in [Jue06], [LSMF06], and [Avo07].

2.3.5.2 Light-Weight Approaches to RFID Tag Authentication

The design of security protocols is a topic that requires careful engineering and strong peer-reviewing before they are widely accepted and considered reliably secure. Research into light-weight authentication protocols for RFID tags only started few years ago, and no mechanism has been widely established yet. Many proposals being made are later found to be inadequate or insecure (e.g., see [DFJ07], [LW07]). Here, we restrict ourselves to approaches that appear to be sound but generally their adequacy to RFID security problems and their practical implementation still need to be proven.

A pseudonym-based identification of tags has been proposed in [Jue04]. Pseudonyms are randomly chosen and pre-distributed to the reader. Due to their randomness, they can identify a tag only to a reader that already knows them. At each query, the next pseudonym in the list is returned (extensions to this are proposed, such as time-triggering). Since there are only a limited number of them, they have to be used only sparingly and need to be updated regularly.

EPC specifies for Class-1 Generation-2 tags a *kill* command that is protected by a password. It allows disabling a tag, but is only available to authorised parties who are able to present the correct password to the tag. In [Jue05a], this capability is turned “upside down” for actually authenticating tags. Usually, the kill command permanently disables a tag; however it is shown how tags can be designed to still comply with the standard and at the same time to not actually execute the kill command. Instead of disabling itself, the tag simply returns a response, which says whether the presented password has been correct or not.

Vajda et al. [VB03] discussed lightweight authentication protocols for low-cost tags. The proposed set of challenge-response protocols comprises simple XOR encryption with secret keys (although also complex encryption like RSA was proposed, it’s not considered here because it is infeasible in low-cost tags [JW05]). The cryptographic

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

problem with keys being static in XOR encryption is addressed by re-keying schemes that make use of keys from multiple previous protocol runs.

A reader that wants to authenticate a tag first queries the tag for its identifier and makes a database lookup for the password. A malicious tag may accept any password presented, and would therefore be able to impersonate any other tag. In order to avoid this, the reader sends not only the correct password but also a number of incorrect ones to the tag. Only if the tag shows the expected behaviour, i.e. for each password the associated response, the tag is authenticated.

The approach proposed in [MW04] involves the computation of a pseudo-random function (PRF), e.g., a hash function, and is therefore more demanding than the previous one. As a benefit, it provides mutual authentication, i.e. the tag is able to recognise illegitimate readers. Here, the identifier and the key are both considered shared secrets. On request, the tag responds with its ID being obfuscated using the key and random nonces. The reader authenticates the tag if the used key matches the ID. The reader then demonstrates its knowledge of both values to the tag, thereby achieving mutual authentication. This scheme, which requires linear effort by the reader for finding the appropriate ID/key combination, is further developed into a tree-based version that reduces the effort necessary for the reader but increases the number of communication rounds between reader and tag.

2.3.5.3 Strong Cryptography for RFID Tags

The major problem regarding the implementation of strong security on RFID tags is the limitation of computational power. This concerns the physical space on a tag and the computation speed. A typical RFID tag may have between 5,000 and 30,000 gates, but only a fraction of these would be available for cryptographic algorithms. For most such algorithms, this is insufficient. In addition, the relatively large number of computation cycles needed for executing a cryptographic operation is contrary to the desired high reading frequency (e.g., 100 tags per second). The required amount of power to perform the somewhat intensive computations for encryption constitutes a third major constraint for strong cryptography in RFID tags leading to a shorter reading distance. Currently, only few commercially available tags support strong cryptographic operations, and it is unlikely that such technologies will be available in high volume, low-cost RFID tags in the near future. The research community has recognised this problem and is working on solutions. Two types of algorithms are in the focus of research: public-key cryptography and symmetric-key cryptography.

Batina et al. [BGK+06] propose Elliptic Curve Cryptography (ECC) for RFID tags. ECC enables public/private key operations similar to RSA, but requires less space since the key length can be much smaller at the same security level. They propose an implementation that consumes approximately 12,000 to 15,000 gates. Instead of relying on a signature-based challenge-response protocol, the authors propose the use of an identification scheme (e.g., see [MOV96]), which is more space-efficient. Still, their scheme is heavily time-consuming and requires between 430 ms and 2.39 s.

The implementation of the Advanced Encryption Standard (AES), a symmetric cipher, on RFID tags is demonstrated by [FWR05]. Their implementation has a complexity of approximately 3,400 gates and requires an area of 0.25 mm² (0.35 μm CMOS). A 128-bit block encryption uses 1032 clock cycles. At the maximum

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

operating frequency of 80 MHz, they achieve a throughput of 9.9 Mbps – at a typical operating frequency of 100 kHz, a block encryption would require about 10.3 ms.

One of the first cryptographic privacy enhancing technologies for RFID is the hash-lock of Weis et al. [WSRE03]. The design principles behind the proposed scheme included the assumption that tags cannot be trusted to store long-term secrets when left in isolation. The authors proposed a way to lock the tag without storing the access key, but only a hash of the key on the tag. The key is stored in a back-end server and can be found using the tag’s meta-ID. This approach can be applied in authentication, namely unlocking a tag would correspond to authentication. However, the cloning resistance of the scheme is based only on the locked state of the tags and so it is more suitable for protecting privacy. Henrici et al. [HM04] have later extended the randomised version of the hash-lock scheme for increased privacy and scalability.

Avoine et al. [AO05] proposed another hash-based RFID protocol that provides modified identifiers for privacy and that can be applied for authentication. In the proposed protocol the authors solve scalability issues of the privacy-enhancing scheme of [OSK03] by introducing a specific time-memory trade-off. In addition, hash-based RFID protocols for mutual authentication have been proposed in [LHLL05],[CLL05],[LAK06]. All these protocols rely on synchronised secrets residing on the tag and back-end server and they require a one-way hash function from the tag. These approaches show how guaranteeing the un-traceability by updating tag identifiers increases the workload of back-end servers.

Texas Instruments has developed RFID based authentication techniques for the pharmaceutical industry. The model presented in [Pea05] is based on authenticating the products through digital signatures that are written on tags. By using TID and a public key, the transponder can be linked to the signer of the data in a provable way. To improve the traceability of tags, the tag memory is also used to store chain-of-custody events.

Juels et al. [JP03] present an approach to increase tracing and forgery resistance of RFID-enabled banknotes by using digital signatures for RFID authentication. The approach uses re-encryption to avoid static identifiers and optical data on the banknote to bind the RFID tag and the paper. Authentication is performed by verifying that the data on the tag is signed using a valid public key. In order to increase cloning resistance, the authors suggest including some distinctive characteristics of the physical media into the signature (i.e. a physical fingerprint of the banknote) and verifying the validity of these characteristics as a part of the authentication process. Zhang et al. [ZK05] have later enhanced the protocol by addressing some integrity issues.

Tsudik [Tsu06] proposes an authentication protocol called YA-TRAP which provides tracking-resistant tag authentication through monotonically increasing timestamps on the tag. YA-TRAP requires a pseudo-random number generator (PRNG) on the tag and its basic version is vulnerable to DoS attacks through timestamp de-synchronisation between the tag and the server. The approach does not require on demand computation for the back-end as a result of a pre-computed hash-table for later tag verification, which means less load for the server than for example in [MSW05]. Chatmon et al. [CLB06] proposed anonymous RFID authentication protocols based on YA-TRAP that provide anonymity for authenticated transponders

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

and address some vulnerabilities of the original design, while increasing the server workload.

Juels et al. [JW05] introduced an approach for low-cost authentication based on the work of Hopper and Blum (HB) [HB00]. The proposed HB^+ protocol makes use of the hardness assumption of statistical “Learning Parity with Noise” (LPN) problem and can be implemented on low-cost tags, as it only requires bitwise AND and XOR operations and one random “noise bit”. The security of HB^+ against active adversaries has gained publicity in the scientific community and is discussed in details in [KS06]. The first version of the [JW05] protocol was found to be vulnerable against a realistic active attack [GRS05]. Proposals to address the security issues have emerged, including the modified HB^{++} by Piramuthu [Pir06].

Dimitriou [Dim06] proposed a protocol that addresses privacy issues and aims at efficient identification of multiple tags. The enhanced version of the protocol is considered here, since the basic one does not protect the tags against cloning. In this approach the tags need a PRNG and a PRF for symmetric-key encryption. The proposed protocol is efficient in terms of tag-to-reader transaction and protects the privacy of transponders by avoiding transmission of static IDs. However, since the tags share secret keys, compromise of one tag may reveal information about others. In another work [Dim05] the author proposes a lightweight RFID protocol against traceability and cloning attacks. This approach bases on a refreshing a shared secret between tag and back-end database and requires hash calculations and PRNG from the tag.

Duc et al. [DPLK06] proposed a communication protocol for RFID devices that supports tag-to-reader authentication based on synchronisation between tag and back-end server. The proposed scheme is tailored for EPC Class-1 Generation-2 tags so that it requires only a PRNG on the tag and pre-shared keys. The approach also takes advantage of the cyclic redundancy check (CRC) function that is supported by Generation-2 tags. The underlying idea is to use the same PRNG with the same seed on both RFID tag and on back-end side and to use it for efficient key sharing. The encryption and decryption can then be done by XORing the messages.

Ranasinghe et al. [REC04] presented ways to implement challenge-response authentication protocols on RFID tags without using costly cryptographic primitives. These proposals are based on a Physical Unclonable Function (PUF) residing on the tag, which allows for the calculation of unique responses using only some hundreds of logical gates. A possible candidate for the cryptographic tool can be found in [LLG+04], in which it is proposed to use the manufacturing variations of each integrated circuit to implement a secret key on a tag. The back-end server needs to store a list of challenge-response pairs for each PUF (i.e. for each tag) because, without encryption, a PUF challenge-response pair that is used once, can not be used again since it may have been observed by an adversary. PUF based security is still an area of active research. Also Tuyls et al. [TB06] proposed the use of PUFs to increase the resistance of RFID transponders against both physical and communication based cloning attacks and defined an offline authentication protocol. The authors estimated that their anti-clone tag can be built with around 5,000 gates.

Engberg et al. [EHD04] proposed so called zero-knowledge device authentication as an answer to consumer privacy issues. In their proposal the tag must authenticate the reader before it returns any traceable identifier. The scheme is based on shared secrets

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

and requires a hash function from the tag. Also Rhee et al. [RKKW05] proposed a challenge-response protocol for ensuring the privacy of users. The proposed protocol does not update the tag ID and therefore can be applied in an environment with distributed databases. The protocol relies on hash calculations by the back-end database, so that the tag ID is the only necessary shared secret between the devices taking part in the authentication.

Molnar et al. [MW04] proposed private authentication protocols for the use of RFID in libraries, that have the advantage that tag and reader can do mutual authentication without revealing their identities to adversaries. The protocols make use of a PRNG residing on the tag. Molnar et al. presented in [MSW05] another privacy enhancing scheme where an RFID pseudonym protocol takes care of emitting a different pseudonym using a PRF each time. In order to relate pseudonyms and real tag IDs, the authors presented an entity called Trusted Center (TC) that is able to decode the tag responses and obtain the tag's identity. In the same work the authors introduced the term *ownership transfer* that refers to a TC giving only permissions to certain entities to read an RFID tag.

Gao et al. [GXW+04] proposed protocols for improved security and privacy of RFID in supply chains. In their proposals the tags store a list of licit readers to protect the tags against skimming and the tags therefore need a rewritable memory. Other tag requirements include a PRNG and a hash function. Though the protocol burdens the back-end server with some computational load, the approach is designed to be suitable for a large number of tags. Yang et al. [YPL+05] proposed a mutual authentication protocol that provides protection against replay and man in the middle attacks even when the reader is not trusted and the communication channel is insecure. This mutual authentication protocol provides privacy protection and cloning resistance, but disadvantages include that the tag must be able to calculate hash functions and that two secrets need to be stored in the tag and in the back-end server.

Most approaches using light-weight cryptographic mechanisms for tag authentication are in an early stage of development. There is not yet any widely accepted, thoroughly peer-reviewed, and generally usable mechanism as of today. Therefore, these mechanisms cannot be recommended for wide deployment. Although some of the novel approaches seem promising, cryptographic authentication should rely on well-established and proven tools instead.

Strong cryptography may become affordable for low-cost RFID tags at some time in the future. However, most useful protocols require more than just one cryptographic operation. For reader authentication, for example, the tag itself must generate a random challenge, which requires a PRNG on the tag or another source of random numbers.

2.4 Copy Protection of Tags

In the preceding section, a number of product authentication approaches were outlined. For most of these approaches, a tag needs to be attached to a product (see Table 2). These tags store data (mostly an identifier) that is used to identify and authenticate products, or they serve as a copy protected feature in the sense of chapter 2.3.2. Examples for technologies employed for tagging products include RFID and barcodes.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Authentication method	Tags used	Importance of copy protection for tags
Direct authentication	No	
Authentication by means of a copy protected feature	Yes	
Verification of unique identifiers	Yes	Important
Plausibility checks of track and trace data	Yes	Less important
Secure object authentication	Yes	Important

Table 2: Authentication Methods and the Importance of Copy Protection for Tags

When product authentication is based on tag authentication, copy protection of tags becomes important. If a product is authenticated based on data that is written on a tag (usually a unique number, e.g. an EPC), it needs to be ensured that the tag and the data written on it can not be copied (see Table 2):

- Direct authentication and authentication by means of a copy protected feature: For these approaches the copy protection of tags does not play a role as no tags are used at all.
- Verification of unique identifiers: If a unique identifier can easily be copied, the system will not be able to distinguish between a genuine product and a copied one. This is why copy protection of tags is important for this approach. If the tags are protected from copying, the approach is effectively secure object authentication e.g. using cryptographic tags. If not, we can assume that this method can detect some but not all counterfeit products, being not perfectly secure.
- Plausibility checks of track and trace data: The logic for making sense of the data read in this case is not on the tag, but rather on the network. Based on a read unique identifier, the logic of the system determines by means of artificial or human intelligence if the product is genuine or counterfeit. The goal of the plausibility check is to determine whether the tag is the genuine or a cloned one, which is how the tag cloning attack is mitigated in this approach.
- Secure object authentication: This authentication method has incorporated cryptographic measures in order to prevent cloning of RFID tags. Certainly, being secured against tag cloning attacks plays an important role to authenticate products based on this approach.

Knowing about the importance of anti-tag-cloning mechanisms for the introduced authentication approaches, in the following it will be discussed how RFID tags and barcodes can be copied and which countermeasures can be applied.

In the context of this section, passive RFID tags are considered. In the case of EPC Class 1 Generation 2 tags, the RFID reader only reads the data written on the tag. The validity of the tags is not checked. This means, a reader cannot distinguish if it reads a genuine or a copied tag as the data is the same. At the same time, a tag transmits its

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

data to any reader that has the technical capabilities to read it. Data written on RFID tags can be gained in the following ways [Jue05a]:

- **Skimming:** The term skimming denotes an attack where the adversary scans an RFID tag retrieving the data stored on it. This attack is sometimes also referred to as clandestine scanning of the tag.
- **Accessing tag database:** Assuming the manufacturer maintains a database containing all numbers that have been written onto RFID tags that in turn have been attached to products, an adversary can also try to illegally access this database and gain valid product numbers from there. In addition, if the tag database is accessible for authentication queries, an adversary might use it as an oracle to find out serial numbers of genuine products through multiple bogus queries.
- **Reverse engineering:** An adversary can clone tags by copying them physically. This means, disassembling the tag, finding out about its physical properties and building a tag that has the same features. Reverse engineering can also include physical attack to a protected memory for example to read the tag's secret key.
- **Eavesdropping:** If a tag provides authentication mechanisms, an adversary can still eavesdrop the communication between the reader and the tag and receive all data that is communicated between the two. The eavesdropping distance of the reader-to-tag channel is longer than that of the tag-to-reader channel due to bigger transmission power. Therefore eavesdropping can be mitigated by using one-time pads generated and sent by the tag that are used to encrypt the following communication. This method is used for example in the EPC Class-1 Gen-2 protocol when transmitting KILL and ACCESS passwords.
- **Guessing valid data:** If products are numbered by a simple scheme (for example sequentially), an adversary can try to guess valid tag data (product serial number).

Knowing that counterfeiters can clone more and more complex products and different security features, we can assume that RFID tags (and any unprotected data) can also be cloned. Cloning RFID tags will become further facilitated with field programmable tags –tags that can be easily written on by devices like mobile phones.

However, cloning of RFID tags can be prevented by the following means:

- **Cryptography:** Cryptographic authentication of RFID tags (section 2.3.5) makes tag cloning substantially harder. Even though the product serial number of cryptographic tags would be unprotected and thus vulnerable to cloning, the secret key of cryptographic tags is hard to copy. Also cryptographic tags, however, can be cloned e.g. by side-channel attacks, reverse-engineering and cryptanalysis, brute-force attacks, or active attacks against the protocol. Also the data on a tag can be protected by a reader-to-tag authentication mechanism where the tag transmits the data of interest only to authenticated and authorised readers.
- **Data-on-network:** The approach of utilizing plausibility checks based on track and trace data sidesteps cloning of tags. It is not a prevention of tag

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

cloning in the classical sense, but rather a reactive measure. It authenticates products using intelligent algorithms to determine if the data read from an RFID tag makes sense in the context where it is read (cf. section 2.3.4). Once there are reliable algorithms for track and trace based product authentication, it will be visible (if a product exists twice in the system) that a clone is on hand. Nevertheless it is not sure that the algorithm will be able to determine which of the products captured in the system is genuine.

- **Combination of security features:** By combining several authentication approaches, the importance of cloning security can be reduced. A product can be equipped with a copy protected feature for authentication, and in addition with a tag for identification.

Although the main focus of this section is on RFID tags, we consider briefly also cloning of barcodes. Simple barcodes provide no anti-cloning features. Many of them can be easily cloned by using standard copying machines. Custom barcodes can also be generated using a broad range of barcode generators that are available on the internet. This is why normal barcodes are a suitable tagging technology only in those product authentication approaches that do not rely on tag authentication. However, as barcodes are printed, they can be superimposed with a CDP or a digital watermark to detect copying.

2.5 Binding Between Tag and Product

This section discusses how a tag that is used to identify and authenticate a product can be associated with a product in an unquestionable way. The binding between a product and different kinds of tags containing information about it is important when it comes to product authentication. This is due to the following simple reason: if a counterfeiter steals a tag from a genuine product and attaches it to a counterfeit, this product will not be recognised as counterfeit any more. It will be treated like a genuine product – thus it tricks the authentication.

The binding between a tag and a product can be established either by physical or by virtual means. A physical binding makes it hard or impossible to separate the product from the associated tag without destroying either one of them. This would usually prevent counterfeiters from re-using tags, which were obtained for example from discarded products, for marking fake products. The physical binding is further elaborated in D4.1.

The virtual binding of products and tags is presented by Nochta, Staake and Fleisch [NSF06]. Product specific features, such as its weight, colour or even an image is converted into digital information and stored on a tag, which is attached to the product. The data can later be compared to the actual product features. If they match, one gets a certain level of assurance that the product is genuine. If there is a mismatch, one definitely encountered a counterfeit.

The assurance level depends, of course, on the chosen product feature, which should be as hard to imitate as possible. Weight, for example, may be well-suited for goods that are made from expensive materials for which a counterfeiter would use substitute materials that would most likely not yield the same values. Another example would be a product fingerprint obtained by laser scanning (cf. section 2.3.1 and deliverable 4.1), which provides a unique fingerprint for each item.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

2.6 Sealing Products

In the preceding section it was found that the binding between tags and products is a fundamental issue when authenticating products. An issue closely related to the binding between tag and product is what is frequently referred to as tamper-evidence or sealing of products.

A seal is a tamper-indicating device designed to leave non-erasable, unambiguous evidence of unauthorised access or entry [Joh05]. Tamper-indicating seals have been used for more than 7,000 years. They are employed to prevent cargo theft, smuggling, tampering, espionage and terrorism.

There are many technologies used to implement seals for products. A promising way to seal products is provided through the use of tags as seals. In this case, the tags (e.g. RFID tags) are mostly attached to the packaging or the container of the product. A typical example is attaching a tag to the screw top of a pill bottle, making it impossible to read the tag once the bottle was opened and its antenna was broken. In the following, a range of practical implementations of seals that are based on tags are described. Non-electronic, i.e. “classic”, seals are discussed in D4.1.

An approach offered by Savi Technology is the use of sensor bolts with embedded RFID tags for the purpose of helping African meat producers to improve the visibility of their containerised cargo [Col04]. In this case, beef is loaded into refrigerated containers and the container is sealed using the sensor bolts. After the transport, the tag is read for tamper-evidence. Then, the container is unlocked and the beef is removed. The sensor bolts are able to detect when a container seal has been tampered with or broken on the way and it stores data about tampering attempts. In addition, the sensors record the identity of the worker who sealed the container.

The Swedish start-up Cypak provides a proprietary, contactless data transfer technology, similar to RFID [Col04a]. According to the company, the technology connects objects to host computers at a fraction of the cost and power consumption of RFID. The technology is employed within the pharmaceutical industry in order to provide tamper-evident packages. Furthermore, it is used by the Swedish Postal Service in a trial to track packages internally, aiming on solving internal integrity problems that occur during the transport of packages. Currently, Cypak works on enhancing the read range of the tags and on adding temperature sensors to their technology.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08



Figure 11: Tamper-Evident Plastic Wrap

The company Pliant has developed a plastic wrap that uses RFID to make pallets tamper-evident [O’C07]. They developed a way to incorporate electrically conductive trace into a stretch film, ergo the plastic wrap. The process is as follows: The film is wrapped a number of times around the goods that are stored on a pallet and is then connected to a battery-powered circuit board, electrically connected to a passive EPC Generation 2 RFID tag. The tag is connected to the circuit in a way that it can only be read when the circuit in the foil is completed. If the foil is stretched or the circuit is interrupted, the tag will not be readable anymore, which means the pallet has been tampered. Companies allegedly interested in the technology are from the retail and from the pharmaceutical industry.

The RFID label manufacturer Avery Dennison and the RFID software and hardware manufacturer RF Code have developed a sealing technology called Secure Strap [RFI04]. It consists of an active RFID locating device attached to a fibre-optic tamper sensor cable, which transmits data to a back-end system in real-time. As soon as the cable is disturbed, the sensor sends an alert to the monitoring system. The device is currently used to monitor overseas shipments of containers.

Mikoh Corp. have designed and implemented a reusable tamper-indicating container called SecureContainer [Lin07]. If the container is opened, the RFID tag attached to it is disabled or alerts a monitoring system, depending on the option chosen by the customer.

To conclude, there are different approaches for sealing product packages depending on the application. The reviewed approaches use different technologies for the implementation of the product seals, but they all include RFID tags attached to the packaging of the products. Moreover, all reviewed solutions are based on one of the following three basic approaches to provide tamper-evidence:

- **Tag breaks when tampered:** In this approach the tag used to seal the package of the product breaks when the package is opened or tampered with. This approach has the advantage that it is cheap and that the tag cannot be read afterwards by unauthorised parties. This can be an issue with regard to customer privacy. A disadvantage of disabling the tag attached to a product

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

when the product is opened is that middle-of-life and end-of-life scenarios that make use of this RFID tag become impossible for the product after opening.

- **Tag sends a signal when tampered:** This approach is based on using tags that actively communicate with a monitoring system in order to notify it about tampering attempts. This method has the advantage that the information about tamper-attempts is made visible to the stakeholders in real-time. The disadvantage of this approach is that it requires active tags that are more expensive than passive tags.
- **Tag stores event when being tampered:** A hybrid approach between the two approaches described above is to use passive tagging technologies to store tampering attempts. The tags are read once the container or product has reached its destination. This has the advantage of being able to use cheap tags while at the same time making visible at which point in time the package of the product was tampered with. A drawback vis-à-vis actively sending notifications about tampering attempts is that the event cannot be transferred to the monitoring system in real-time.

2.7 Status Verification

The status of a product helps to describe at which point of the lifecycle a product currently is. In some cases, in addition to authenticating a product, it is important to verify that a product does not have an unacceptable (or incorrect) status. The advantages of a status verification of products and how this contributes to a safer and more secure supply chain becomes evident when considering products with an unacceptable status. In their analysis of threats to the pharmaceutical supply chain, [KSCB03] mention “expired”, “discarded”, “sample”, “returned”, and “recalled” as examples of an incorrect product state. Similar status violations can be found in other industries, e.g.:

- A bottle of milk that is past its sell-by date
- A car brake that has been recalled
- A gadget that is sold in Spain but has an Italian manual attached
- A spare part that was flagged for disposal but is mounted on a plane instead
- A deep-frozen fish whose cold chain was interrupted during transport
- A handbag that was destined to be sold in Hungary, but is sold in Germany instead, or
- A stolen watch that is offered for sale

In each case, the product status violates a condition that is necessary for the proper trading, use, or consumption of products. The issues listed above either threaten the safety of consumers or negatively affect the revenue and compliance goals of companies and are therefore listed by industry representatives as pain points ([PSR04], [PSR05]).

Verifying the status of products according to a predefined set of rules is, at first glance, not related to product authentication. We address this problem in this report because the ultimate goal of companies is to ensure the security and safety of

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

products. This implies that the product quality must be acceptable and that products with a wrong status must be eliminated from the supply chain even after the shipment [Ina06a]. Second, the necessary product checks can be carried out with the same infrastructure that may be used for product authentication. A track and trace infrastructure like the EPCglobal network is needed to get the information necessary for performing the status checks listed above. In fact, many of the commercial authentication products offer functionalities such as recall and returns management¹¹ or an integrated check of the expiry data [Ver05].

All status checks have a similar pattern: at design time, acceptable discrete values or ranges of values are determined and, if necessary, annotated with additional conditions. At runtime, the actual values are compared to the acceptable values and an appropriate action is taken if a condition is violated. The following types of checks can be distinguished:

- How often does the product status change: static, dynamic, and semi dynamic data?
- Who determines the status change: brand owner, actual owner, or the product itself?
- When are the status changes detected: immediate (real time) or delayed detection?

[KSCB03] introduces a distinction between static, semi-dynamic, and dynamic data in the context of status checks. Static information such as weight, size, or expiry data does usually not change during the lifecycle of a product. Today, this type of data might be printed on the product or its packaging during manufacturing. Semi-dynamic data changes with long time intervals. This category of data comprises lot numbers based on production runs as well as information about the recall or theft of a product. Dynamic information changes within short time intervals and includes location, temperature, and other parameters that are typically captured by sensors. Checks may be complicated in case the status of products changes after the goods have left the premises of the brand owner or manufacturer, e.g., when they are stolen, discarded, or recalled. Nevertheless, it should be possible to inform the current user or prospective buyer about the proper actual status of a product. Furthermore, [Ina06a] distinguishes between status changes that are determined more or less immediately, e.g., the mishandling of products during transport or the expiry of products, and status changes that have negative consequences now but will only be detected in the future, e.g., contaminated drugs that cause diseases with long incubation periods.

An infrastructure for gathering the relevant data for most of the status checks was described in section 2.3.4, in which it was detailed how product authentication can be achieved by checking the plausibility of track and trace data. In order to perform a status check, the tracing system must capture – besides the plain tracking data needed for authentication – the additional object information necessary for the check [Ina06a]. Static data like the expiry data or the country in which a product should be sold can be stored in the local database of the brand owner at manufacturing time. Alternatively or additionally, the data can also be written on an RFID tag that is attached to the product. The object information stored on the tag must be protected

¹¹ <http://www.supplyscape.com/products/pedigree/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

against tampering – for example changing the expiry date - which can be achieved with message authentication codes (MAC).

If a data-on-network approach is chosen, the brand owner can make the additional object information available to supply chain partners via the EPCIS interface. By using the ONS or the DS, an interested company will be able to determine where it can get the information it needs for performing a check. Thus, any interested party that has appropriate access rights can automatically check whether the status of a given product is acceptable. If information about licit distribution channels is entered by the brand owner and given that the product location is read and published in the EPCglobal network, an application based on the EPC data is therefore capable of detecting grey marketing, parallel trading, and illegal product deviations by comparing the actual location of a product to its intended point of sales.

The EPCglobal network or a track and trace application with a similar distributed architecture is also well suited for dealing with status changes that happen after a product was released to the supply chain or sold to the end-customer. In the EPCglobal network, the EPC manager usually stores static and semi dynamic information about its products in a local database [KSCB03]. The EPC manager might update the status information in case of recalls, withdrawals, or theft and flag the product as unacceptable [HMBM03]. As every query for a specific product is routed by the ONS to the EPCIS server of the EPC manager, a requesting party may be supplied with up-to-date status information, e.g. indicating that a product is flagged as stolen and should not be sold. Furthermore, the EPC manager will be able to propagate the information about a status change in the network and to locate some (or all) affected items. The manager might notify all parties that are currently in possession of a recalled product [HMBM03].

Products might be damaged or perish during storage or transportation and thus become unacceptable [TRB03]. This type of status change is best captured by sensors that measure, e.g., the temperature, humidity, or pressure that affect products. RFID tags can be augmented with sensors, thus enabling products to capture data about the condition they are in by themselves [BSI04b]. Alternatively, sensors can be attached to sets of products, e.g., a pallet or a truck load [TSM01]. Either way, the recorded measurements can be checked against allowed ranges of values in order to determine whether products are in an acceptable state and can safely be consumed or used.

2.8 Privacy protection

Many concerns have been raised around the traceability of RFID tags, since this may potentially lead to privacy breaches. In general, it is possible for everyone to interrogate RFID tags with standard hardware and at least read their – fixed – identifiers. When the same identifier is encountered at different locations, tracing information about the object bearing the tag can be compiled. Tags on consumer products could therefore lead to the disclosure of movements of people.

In addition to the recognition of formerly encountered tags, additional information about the bearing objects can be retrieved either by decoding the tag identifier itself or by querying databases, using the tag identifier as the key. In the case of EPC tags, they carry structured identifiers that encode information about the manufacturer, the product type, and the product serial number. Such data alone already gives a good idea about the nature of the object, for example whether it is a pharmaceutical

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

product, a contraceptive, a household appliance, a high-valued TFT monitor, or a sweet snack. Depending on the circumstances, this information may be considered sensitive. By querying a database, additional information may be possible to retrieve, such as the manufacturing or sale date, servicing information, or information about former owners.

These issues raise privacy concerns on the level of individuals and confidentiality concerns on the business level. They have to be adequately addressed in order to facilitate the acceptance of RFID tags throughout all industries. We are now going to discuss the existing approaches that mitigate these concerns. Several approaches to the problem have been proposed, with varying implications. In general, all approaches have to provide a trade-off between the utility of tags and the protection of privacy and confidentiality. On one hand, the tag should be readily accessible for legitimate applications, and on the other hand the information carried directly or indirectly by the tag should be protected against unauthorised retrieval.

Many of the authentication protocols discussed in section 2.3.5 try to achieve privacy by disclosing the identifier of a tag only to a reader that already has a predetermined relationship with the tag. Such a solution works well in closed systems, where predetermined trust relationships exist and the device infrastructure is under central (or coordinated) administration but still requires some administrative overhead and limits flexibility. In open systems, it requires an elaborate infrastructure that is comparable to a Public Key Infrastructure. This is an additional effort that requires significant investment.

Other approaches to RFID privacy allow a user to explicitly enable or disable access to her tags. The simplest method is disabling the tag, either permanently or temporarily. This is a radical measure, since it may deny a legitimate user the services provided through the tag. Re-enabling access, if possible at all, requires additional effort from the user. First of all, the (legitimate) user must be aware of the presence of a disabled tag, and must then apply a certain measure to re-enable the tag. Examples in the literature for such measures are the *kill* command [Jue05a], which disables a tag permanently, and clipped tags [KM05], where the antenna is separated from the RFID chip.

A different approach is to block access to the tags on a low level, i.e. on the physical communication layer. This could be accomplished through the use of an RFID detection and jamming device [RCT05]. The device would recognize an active RFID reader and immediately start jamming the used frequencies. Thereby, it would not be possible for the reader to obtain any data from tags that are in its range. The problem of such an approach is that the jamming device needs to be present at all times, which may not always be possible.

Blocking can also be achieved on a higher level, in particular the singulation protocol. The singulation protocol is required in RFID systems in order to be able to distinguish between all present RFID tags. Tags are not synchronised, so if there are two or more tags in reading range, their messages may overlap and make them illegible to the reader. This is resolved by a singulation protocol. One common protocol is the binary tree-walking protocol, which successively asks tags to respond only if their identifier matches a given prefix. By increasing the length of the prefix by one bit at a time, the reader is able to distinguish all present tags after a number of reading rounds. The blocker tag [JRS03] easily defeats this protocol by always responding, regardless of

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

the given prefix. Thereby, the reader is forced to go through all possible prefixes (which is usually impractical and would be terminated after a certain time) and would be led into thinking that for each possible identifier, a tag is present. This is obviously incorrect, but the reader has no means of distinguishing real tags from the blocker tag, so no presence information is actually disclosed.

A common approach is to limit access to tag identifiers in the time dimension. Instead of immediate, complete feedback upon inquiry, a tag reveals only part of its identifying information [LM07]. If a tag is unknown to a user, the user has to spend some time until the complete information is received. For a legitimate user, this incurs some overhead but doesn't limit applicability. The next time the tag is interrogated, the small amount of initial information is sufficient to identify the tag. However, for attackers such an approach is deterring in many cases as they have to spend some time until they receive useful information while being exposed and under risk of detection. Tags using this approach are not on the market yet as the research field is still evolving.

Most research in RFID privacy focuses on the prevention of tracing, as this is the most important problem for individual people. In a business context, it may be sufficient to retain a level of confidentiality that ensures that detailed product information is not immediately revealed to an attacker. For example, the tag identifier may be openly transferred upon interrogation. However, additional information to the bearing product is only retrieved through a separate interaction that requires authentication, for example through a back-end system. If this extra step has been done once already, the associated information will be readily available for future operations.

2.9 Dependability of Network-Based Approaches

Plausibility checks and statistical analysis of trace data are an effective technique to authenticate products. However, some additional considerations are required to establish a reliable solution on these grounds.

We have to evaluate whether current infrastructures following the data-on-network paradigm cope with the challenges that huge amounts of event data entail, e.g., reliability, scalability, and security of the infrastructure components involved. In addition to these technical issues, business intelligence and integrity risks due to the sharing of event data have significant influence on the completeness and thus on the usefulness of trace data for product authentication.

2.9.1 Network Performance Risks and Bottlenecks

Choosing the data-on-network paradigm such as EPCglobal's approach for track and trace-based product authentication brings forward the classical issues faced in network dependant applications. These include availability, confidentiality, integrity, and reliability. Such issues are always available and we will have to take them into consideration. Since no guarantee can be reached regarding an optimal network performance on these criteria, we have to take measures to mitigate the problems and not have the solution focused on track and trace plausibility checks as the only way of product authentication. As other solutions that are not based on track and trace are discussed elsewhere in this report this section deals with the non-functional

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

requirements of network-based solutions, such as availability, confidentiality, and reliability.

2.9.1.1 ONS

The entry point for cross-enterprise event queries within the EPCglobal architecture is the Object Naming Service (ONS) root service operated by EPCglobal itself. It is obvious that the reliability of this component is crucial for the operation of the whole network like the Domain Name System (DNS) is for the Internet. Because of these similarities it is no wonder that ONS is implemented as an application of DNS as an EPC is converted to an Internet Domain Name in the `onsepc.com` domain. This has several implications [EPC05c]:

- To increase reliability and scalability, the Root ONS service and Local ONS services can be implemented by multiple independent services, as DNS allows more than one server to be listed as a DNS service provider for a domain name.
- The Root ONS service is actually itself two levels down in a hierarchy of lookups, as it has its roots in the worldwide DNS root service.
- ONS benefits from the DNS caching mechanism.

As the DNS so far has proved to be sufficiently robust, we can expect the same from the ONS. In the future the EPC Discovery Service will replace the ONS as a means of finding relevant EPCIS servers. ONS does not adequately support cross-enterprise event queries since the information returned from ONS gives only high-level information on data providers but does not support automatic retrieval of the data itself.

2.9.1.2 EPC Discovery Service

Because the EPC Discovery Service (EPC DS) has not been fully specified yet, it is naturally impossible to form a definite conclusion about its reliability and scalability. But there are efforts in another EU research project, namely BRIDGE, to specify the EPC Discovery Service. The major role of this component would be to indicate all EPCIS repositories that hold information about a particular EPC. This implies that the EPC DS has to communicate to a potentially large number of distributed repositories for each EPC query, which makes the issue of scalability of utmost importance. The work groups in BRIDGE are addressing these issues when comparing the alternative designs of an EPC DS.

Possible alternatives of the EPC DS design include a directory look-up approach and a query relay approach. In the directory look-up approach, the client queries the EPC DS for an EPC number, the EPC DS replies with the EPCIS repositories that hold information about the particular EPC, and the client then queries these EPCIS repositories on its own. In the query relay approach, the EPC DS has the more limited responsibility of forwarding the queries to the appropriate EPCIS repositories. From a *scalability* point of view, the *query relay* approach is a clear winner. This is because the task of the EPC DS would be simply to forward queries and not calculate and send the replies. It would also support the organic growth of the number of clients connecting to the EPC DS, especially because new clients do not have to get the consent of the whole community using this EPC DS before getting connected. As for

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

the issue of *reliability*, the *directory look-up* approach seems like a better solution because it is the responsibility of the client to manage connections and get responses from the EPC DS and the EPCIS repositories. So in the case of a faulty connection with the EPC DS or one of the EPCIS repositories, the client would miss the reply and try to connect again. In the query relay approach, the client would send a query to the EPC DS and wait for separate replies from the EPCIS repositories. If one of the EPCIS repositories is down the client cannot know which, so it cannot try again later because it assumes that what it received is a complete set.

As we saw, scalability and reliability may be at odds with each other, different design scenarios favouring one but not the other. For our practical cases, we may prefer supporting different solutions in different scenarios. For example, in certain supply chains in which a dominant player exists, the problem of scalability can be inherently mitigated since the connected repositories are known in advance. This way we can pick the design that emphasises reliability and get better reasoning from all EPCIS repositories. In less controlled supply chains, the situation is more complicated and it would be impossible to limit the number of connections to the EPC DS or to know them a priori. In this case we should opt for a design that favours scalability, thus sacrificing reliability and taking this into consideration in our solution. The latter would then not depend on having a complete record from all EPCIS repositories but would reason about track and trace data from the available connections only and discard the EPCISes which do not reply to the query.

2.9.2 Security

2.9.2.1 ONS

If a system like the EPCglobal Network is used as the basis for trace data analysis, securing the infrastructure from attacks is of utmost importance. Such a system has to be protected against these main types of attacks:

- Denial-of-service attacks attempting to make the EPCglobal infrastructure unavailable to its intended users
- Attacks attempting to compromise the lookup service
- Attacks attempting to compromise data accessible via the EPCglobal infrastructure

As stated out earlier the ONS Root Server depends on the DNS root service and is thus susceptible to the same attacks. The last attacks on all 13 root DNS servers took place in 2002 and 2007. However, the attacks were not able to disrupt the entire system.

Attacks attempting to compromise the lookup service, like spoofing attacks or DNS cache poisoning, aim at falsifying lookup data that clients assume to be authentic. These problems are tackled by two security protocols: Secret Key Transaction Authentication for DNS (TSIG) and Domain Name System Security Extensions (DNSSEC). These protocols likewise enhance the security of ONS.

2.9.2.2 EPCIS

Bindings of the EPCIS Capture Interface or the EPCIS Query Control Interface may provide a means for the EPCIS server to authenticate the client's identity, for the

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

client to authenticate the EPCIS server's identity, or both [EPC06a]. Based on the client's identity a server can thus make a decision whether capture or query operations are permitted or not. With respect to the Query Control Interface an EPCIS server may decide to provide access to only a subset of information, depending on the identity of the requesting client.

2.9.3 Business Intelligence and Privacy Issues

Plausibility checks and statistical analysis of trace data only work if access to this data is granted. The problem is that companies generally are reluctant to share data as they consider them as trade secrets and it is unlikely that access to trace data of products will ever be available to the broad public. Instead it is more realistic to expect that only required subsets of trace data will be shared between companies bound by contract. Another option is to develop a mechanism in which companies which do not have a contract in place but require access to each other's data in real time can automatically negotiate on a contract that governs the data access between them. Such mechanisms are found in the literature under the name Automated Trust Negotiation (ATN) because their goal is to establish trust between partners which do not know and thus do not trust each other beforehand [WN02]. It is a future research task to develop the concept of ATN for the exchange of item-level event data in business systems, which is beyond the scope of the SToP project.

2.9.4 Discussion

Plausibility checks and statistical analysis of trace data might turn out as an effective technique for authenticating products. At least, they can be seen as an additional security layer in combination with the authentication of security features. A verification infrastructure based on the data-on-network paradigm has to fulfil certain requirements with respect to availability, reliability, and security. With respect to the EPCglobal architecture, the Object Naming Service seems to cope with these challenges as it is based on the robustness of the Domain Name System. EPCIS repositories would be typically run by product manufacturers, and these are responsible for providing a reliable system that is available for remote access when needed. The intra-enterprise EPC Discovery Service that connects different EPCIS servers relies on an available network connection and thus faces the sometimes conflicting issues of reliability and scalability. Different scenarios may require different designs which favour either scalability or reliability of the EPC Discovery Service.

2.10 Combined Authentication Approaches

Some of the authentication approaches discussed in the previous sections can be combined in order to raise the respective level of security. Deliverable 4.1 discusses approaches for combining different authentication methods. These range from integrating multiple independent features that are not connected whatsoever, to linked features that encode and protect shared information, up to interacting features where the utilization of one feature is required in order to use the other. In this context, Deliverable 4.1 also discusses certificates that interact with a public key infrastructure (PKI).

While the realization of combined authentication approaches imposes certain challenges regarding physical feasibility and costs, it will also have an effect on the

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

requirements for the software development of the Product Verification Infrastructure (PVI). As long as individual features are not totally integrated and depending on each other, it will be necessary to provide a highly flexible rule-based or probabilistic authentication solution that is capable of adapting to and dealing with ambiguous, contradicting, or partially missing information from the individual features and draw respective conclusions depending on the required level of confidence.

Consequently, the PVI development activities will take combined authentication approaches into account. The corresponding system design will be elaborated in a later deliverable of WP3.

2.11 Analysis and Comparison

In this chapter, we have outlined how items can be identified and have presented five approaches to authenticating products. We have analysed methods and technologies suited for verifying the identity of products and considered their applicability in various domains. A more detailed analysis of the applicability of technologies will be presented in chapter 4, in which we investigate how suited certain approaches are for different industries. We will now revisit how the presented additional concepts like tamper detection and binding tie in to authentication and subsequently compare and evaluate the illustrated product authentication approaches.

As we have described, authentication can be based on natural product properties, on an artificial feature or on a tag that stores data, e.g., an identifier. As pointed out in section 2.4, a tag that carries an identifier needs to be copy protected, because if it is not, a counterfeiter can intercept the identity and pass it on to one or more counterfeit products. If the tag itself is not guarded against copying, a duplicate detection can be implemented in a data-on-network approach, but this will likely be less secure than protecting the tag data directly.

Ensuring the binding between a tag and a product is irrelevant for direct authentication as no tags are involved in this approach. For all other approaches, it depends on the type of tag used and on its position relative to the product whether additional *binding* mechanisms need to be implemented. If a tag is integrated inside the product, binding is usually achieved automatically. The binding between a tag and a product can either be based on mechanical principles (e.g. on RFID tags losing their functionality if they are ripped off) or it can be ensured virtually by personalising the tag. This is achieved by writing a (ideally) unique property of the product to the tag, and it requires an additional verification step.

Anti-tampering measures have to be considered in particular if the tag is not applied directly to the product, but to its packaging. In this case, binding mechanisms will only ensure that the tag stays with the packaging, but it must furthermore be ensured that the product stays with the packaging and that the product is not changed. Therefore, appropriate sealing mechanisms need to be employed.

Status checks will help to ensure product safety and to detect deviated goods, but they will not increase the reliability of authentication. Status checks can be implemented in addition to authentication if a track and trace system is used or – in case of static data – when using tags that are able to store additional object data.

Because of the wide range of possible approaches and technologies for product authentication, there is a need for a sound comparison of the different approaches.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Which approach is the best in a given situation depends on the goals pursued, on the products to be checked, on the industry, and on the entire set of circumstances in which the technology should operate. Based on the findings so far, we provide a comparison of approaches presented. As the authentication approach (e.g., track and trace based check) alone cannot be used as unit of comparison because much depends on what technology is used to implement the approach, we decided to employ a combination of authentication approach and enabling technology as the basic unit of comparison.

Evaluation criteria for anti-counterfeiting technologies can be found, for example, in [KSCB03], [STF05] and [NSF06]. We picked the most selective criteria for comparing the approaches described in this report. We evaluated methods by their general security level, i.e. how reliable the authentication is, the verification speed per item, the variable and fixed costs associated, the maturity of a technology, and whether the authentication can be performed by the customer. The variable costs include the costs for tags and the tag integration cost as well as the costs for measuring a reference value at manufacturing time. Fixed costs comprise the costs for the needed infrastructure. The maturity level ranges from research prototypes (1) and commercially available products (2) to the widespread use of an approach in the real-world (3). Whether a technology can be employed by end-customers or not is evaluated based on the availability of reasonably priced devices for performing the check. These devices include RFID-enabled mobile phones, mobile phones containing a camera (for checking CDPs), and websites allowing customers to enter an identifier they found on a product for verification.

We grouped technologies wherever possible to ensure that unnecessary details are not included in the comparison. We furthermore focused on the most relevant technologies, and, in case of authentication by means of a hard to reproduce feature, can only give examples as this authentication approach is out of the scope of this report. We use three and five point ordinal scales to evaluate the technologies and a field for yes or no in case of end-customer enabled checks. One point means that the technology is ranking comparably low in this dimension (e.g., is slower or more expensive), three and five points meaning that the technology ranks good in this dimension. The use of an ordinal scale implies that a technology that is ranked higher is better than a technology ranking lower, but we do not state to what degree it is better. The extensive analysis required to come to such conclusions is not part of this deliverable.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Authentication Approach	Technology	Security Level (1-5)	Verification Speed per Item (1-3)	Variable Costs (1-3)	Fixed Costs (1-3)	Maturity (1-3)	Usable by Consumers
Direct Authentication	Photo Comparison (manual)	1	1	1	3	3	Yes
	Forensic Analysis (e.g. Chemical)	5	1	1	2	3	No
	LSA	5	2	2	2	2	No
Authentication by Means of a Difficult to Reproduce Feature	CDP	5	2	3	2	2	Yes
	Taggants (e.g. Chemical, DNA)	4	1	2	2	3	No
Verification of Unique Identifiers	Barcode	2	2	3	2	3	Yes
	RFID	2	3	2	2	2	Yes
Plausibility Check of Track and Trace Data	Barcode	3	2	3	1	2	Yes
	RFID	3	3	2	1	2	Yes
Secure Object Authentication	RFID	5	3	1	2	1	No

Table 3: Comparison of Authentication Methods

Although we chose to perform a coarse grained comparison of technologies and approaches, it is evident from Table 3, that there are two distinct groups of authentication methods that complement each other. On the one hand, plausibility checks of track and trace data as well as the verification of unique identifiers are, regardless of the technology employed, well suited for checking large amounts of products quickly. However, only an intermediate security level can be reached with these checks. On the other hand, there are technologies and approaches that promise to be very reliable and can be used as evidence in court. But those methods require a longer verification process that cannot be fully automated and that does not allow for multiple products to be checked at a time. It may therefore be advised to combine a track and trace-based plausibility check, which detects suspicious goods, with a second, more reliable technology in order to detect counterfeits quickly and reliably.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

3 Commercially Available Authentication Infrastructures

3.1 Introduction

In the previous chapter we described different authentication approaches with more emphasis on software-based systems than on direct product authentication. In this section, we will look at commercial products that implement those approaches and offer them as solutions. We will also focus more on software-based systems, but present a number of solutions that are based on product-inherent features or copy-protected tags. The survey presented in this chapter is not meant to be complete, especially regarding hardware-based approaches which are presented as examples of the available products on the market.

The information about the reviewed approaches is mostly gathered from publicly available sources on the companies' websites. In some cases, especially when there was a lack of relevant information, we contacted the companies for more information. The companies that agreed to provide us with the information did that either via e-mail or in short interviews. This chapter focuses on describing the products by mentioning their distinctive features and weaknesses regarding anti-counterfeiting. In many cases there is not much information available about the product, including its known limitations and price, since the companies choose to withhold this data.

The described products are listed in alphabetical order of the name of the company that offers them. Links to the websites of the solution providers are provided in footnotes.

3.2 Products

- Advanced Coding Systems

Advanced Coding Systems¹² (ACS) offers products for product authentication, track and trace, and securing documents. The authentication solution is AuthentiFiber which comprises a unique magnetic signature which cannot be erased, rewritten, or forged. AuthentiFiber can be incorporated into a tag or integrated into the product or the product's packaging. The code can be read - without the need for line-of-sight - through various packaging materials including non-ferromagnetic metals. The DataFiber solution offers, in addition to authentication, track and trace information such as ID, batch number and expiry date.

- Aegate

Aegate¹³ uses mass serialisation with RFID or (1D or 2D) barcodes to enable authentication of pharmaceutical products. Authentication of medicines takes place at item level via a scanner that is connected through a secured broadband link to Aegate's systems. Scanning the products can take place using existing barcode scanners or by installing Aegate scanners. Confirmation of authenticity is returned through the company's existing pharmacy software system.

- AlpVision

¹² <http://www.acs-coding.com/>

¹³ <http://www.aegate.com/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

AlpVision¹⁴, a solution-provider for brand and document protection, offers Krypsos, a server-based authentication system that can encompass several security layers. It includes the Cryptoglyph which uses covert copy-protected security features for authenticating products. The Cryptoglyph uses package markings that are invisible to the human eye and can be printed with available printing equipment, so there is no need for investment in additional hardware. The marking consists of coded fields of dots which can be printed using standard ink but are so small that they cannot be detected by the human eye. The markings are generated by a trusted party and integrated into the package and are then verified by scanning and analysing embedded information. The Cryptoglyph uses a 128 bit-strong encryption. Another product which can be included in the Krypsos authentication system is Fingerprint which uses product-inherent features for authentication. The solution is based on comparing digital images of the original product stored in a secured database with images of the product at hand. Based on image-processing algorithms, Fingerprint authenticates an original product, detects a counterfeit, or fails to determine the outcome.

- Authentix

Authentix¹⁵ is a provider of product authentication technologies that range from security markings to unique identification and tracking. Authentix Serialized Authentication Solution is a system that applies serialised codes to individual items and then aggregates the data into that of their parents: boxes, cases, and pallets. At the different points of shipment and distribution in the supply chain, the unique codes are scanned and the products' authenticity is verified. Authentix also offers authenticity tests based on products' inherent features. This test comprises exposing spirits or drugs to a liquid vial that would leave different markings if the product was original or counterfeit.

- Axway

Axway¹⁶ offers a drug electronic pedigree solution called Synchrony ePedigree. Synchrony ePedigree automates current paper-based processes intended to prevent counterfeiting and safeguard the drug supply. The solution enables companies to link physical inventory movements with B2B transactions, such as purchase orders, ship notices and invoices.

- Certicom

Certicom¹⁷ offers an RFID-based product authentication solution based on cryptographic approaches. A 256-bit digital signature is generated, using the product manufacturer's private key, from the concatenation of the tag unique identifier and the EPC number. This unique signature is written on the tag in the manufacturing line and is used later to authenticate the tag anywhere in the supply chain. The digital signature scheme used is the Elliptic Curve Pintsov-Vanstone Signature (ECPVS) scheme which is based on Elliptic Curve Cryptography (ECC). Its advantage is the compact signature when compared to other algorithms like RSA, thus being more suitable to be written on RFID tags. In order to authenticate the tags, readers need to employ an authentication agent that verifies each signature and recover the encrypted Product Class ID.

¹⁴ <http://www.alpvision.com/>

¹⁵ <http://www.authentix.com/>

¹⁶ <http://www.axway.com/>

¹⁷ <http://www.certicom.com/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- CounterFight

CounterFight¹⁸ provides product authentication based on mass serialisation and track and trace technologies. Counterfeit or diverted products can be identified via verification on the internet or mobile phones. Mass serialisation is based on random unique numbers that are generated using encryption technologies which makes it difficult for counterfeiters to guess what a viable number might be. The unique codes are generated in real-time on the production line – to insure against theft – using the CounterFight Printer Controller (CPC).

- Dintag Corporation

Dintags (Database of Identification Number TAGs) consist of two numbers: an overt and a covert one. To protect a product it is marked by a paper Dintag label which holds these numbers. The overt number is visible and in clear text on the tag while the covert number is hidden inside the tag and can be read only if the label is opened by removing a paper strip. Information on dintagged products is forwarded from the manufacturer to the DINTAG service administrator that links the product ID numbers and the covert numbers that are used in authentication. Consumers (and anyone else) can authenticate a protected product by opening the label and entering the covert number into Dintag's website¹⁹. The web service responds whether the product is authentic or not depending if the correct covert code is entered. The weakness of this approach is that a product can be authenticated only once, that is the first time the covert code is entered on the website.

- FractureCode

FractureCode²⁰ Corporation delivers solutions for the identification and tracking of products throughout their lifecycle down to individual item level. The FractureCode system is based on a unique code, down to the size of 1mm², made up of lines generated in a random order. The code is unobtrusive and can be overtly or covertly integrated into the product design. The codes are applied onto the product, decoded, and stored at a rate of 32 items per second. The code can be used further down in the supply chain for authenticating the products. FractureCode is used in various markets, including pharmaceuticals, tobacco, fast moving consumer goods, identity documents, stamps, currencies, and other security documents.

- Hyperlabel

Hyperlabel²¹ offers a tagging and digital signature solution that combines serialisation and product authentication. Hyperlabel uses an optical tagging technique in which small tags, visible only in infrared light, are printed over the entire package or specific label. There are thousands of tags on a single package or label, each containing three components: an EPC number for unique identification, a digital signature for authentication, and the unique x-y coordinates of the printed tag that can be used to provide the customer with different kinds of product-related information. The EPC number and the digital signature are the same on all tags of one item but the x-y coordinates naturally change. The printed layer of tags has no impact on packaging design and, unlike RFID, Hyperlabel ink is also suitable to authenticate products with metal or liquid. Hyperlabels can also be applied to cash or documents. Line of sight is

¹⁸ <http://www.counterfight.com/>

¹⁹ <https://www.dintag.com/dintag/app>

²⁰ <http://www.fracturecode.com/>

²¹ <http://www.hyperlabel.com/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

required to scan these labels, which doesn't allow for bulk processing like RFID, but, as opposed to barcodes, products can be scanned anywhere on the package and from any angle because the tags are all over the package. The digital signature is based on public key cryptography and is unique per item. Combined with track and trace, a digital signature enables the authentication by different parties. The cost per tagged item is very low but a special reader device is needed to read the tags.

- IBM

IBM offers the so called RFID information center as part of WebSphere²², along with solutions that use it to add value to businesses. Among these solutions are shipment verification, pharmaceutical track and trace, electronic pedigree, and product authentication. WebSphere is compliant with the EPCglobal EPCIS 1.0.

- Ingenia

Ingenia Technology²³ developed the Laser Surface Authentication system (LSA) which authenticates products based on their unique surface. How this technology works is described in detail in deliverable 4.1. In short, the product surface is scanned using a laser beam and from the random patterns and imperfections of the surface, a unique number is generated by the scanner, which can be stored in a database and used later for comparison in order to authenticate a product. The strength of LSA is that the generated sequence of numbers is virtually unique to the object and cannot be faked because it is a totally intrinsic property of the object. The laser beam is also cheap and scanning can be easily integrated into the production processes. Even when the surface is subjected to damage and wear, the object can still be identified because the surface analysis works on a microscopic scale and tampering cannot happen on such small scales. The problem with using LSA for mass authentication is that it uses a beam, thus the need for a direct line of sight. Furthermore the product to be scanned should have a fairly flat and non-reflective surface for the scanning process to give a meaningful result.

- Kezzler

Kezzler²⁴ is a provider of product authentication and secure track and trace software solutions to the pharmaceutical and the fast moving consumer goods industries. The product authentication software system they offer is based on uniquely identifying items by proprietary codes called kezzlercodes. These unique, random codes are generated by Kezzler's encryption engine and the product IDs are not stored in a database, thus protecting the process from attacks on the IT infrastructure. Instead, kezzlercodes are self-contained and deciphered on demand by the kezzlercode encryption engine (called Intencor SSP). This particular technology makes the security code generation and subsequent authentication of the product IDs extremely fast and scalable. Coded items can be authenticated via the Internet, SMS, PDA, or WAP. Compass, the secure track and trace (technology) solution they provide, uses the same codes and provide even item level localisation and aggregation information to the brand owner. Making use of different levels of aggregation information (packaging hierarchies), the database entries that need to be stored are minimised and item level information can be deduced without duplicating the same information for each distinct item. This is also the basis for other related business process propelled by the same

²² <http://www-306.ibm.com/software/data/masterdata/rfid/>

²³ <http://www.ingeniatechnology.com/>

²⁴ <http://www.kezzler.com/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

product ID, for instance product recalls. The solution is managed by the brand owner and protects the products by remote control – thus enforcing the brand owners’ supply chain policies.

- Microtrace

Microtrace²⁵ offers several taggant technologies, most notably the Microtaggant identification particles. These particles are microscopic, traceable, and highly versatile in their use and application. In their basic form, Microtaggants are a unique numeric code sequence in a multiple coloured layer format. In more complex forms, Microtaggants deliver multiple layers of security through the incorporation of several taggant technologies.

- Orbid

Orbid²⁶ is the company behind 2DMI (2 Dimensional Mark Identification), a marking technology that provides products with unique codes that enable them to be tracked and traced. 2DMI provides to each product a unique printed mark that can vary in size depending on the application and can be applied to different kinds of materials. The mark is generated after encrypting a desired data string (serial number, production date, etc.) into a unique 2DMI code. The printed code can then be applied on the product, either by printing on a label or by laser marking directly onto the product. The original data can be retrieved by scanning the 2DMI code with available equipment.

- PackAgent

PackAgent²⁷ from Stora Enso and Trackway is a software solution for product authentication and track and trace based on unique identification of items. The supply chain partners share the item level information according to business rules, so the assumption is that the supply chain partners are known beforehand. The partners update item-level information throughout the supply chain, and this track and trace data can also be used to generate an electronic pedigree. The identification technologies that are supported include (1D and 2D) barcodes and (HF and UHF) RFID tags. Stora Enso carried out a successful pilot project that used PackAgent in a pharmaceutical supply chain.

- RainingData

RainingData²⁸ provides the TigerLogic ePedigree solution. TigerLogic ePedigree comes with the out-of-the-box functionality required to meet the drug ePedigree regulations. It will accept an electronic pedigree with the drug shipment from the supplier, accept custody with an electronic signature, manage the pedigree within the organisation and record the revised pedigree sent to the customer. All of this data is encrypted. The TigerLogic ePedigree system has an ePedigree bank, which allows pedigrees to be divided and allocated to multiple containers. The system supports paper pedigrees, electronic pedigrees, RFID and barcodes.

²⁵ <http://www.microtracesolutions.com/>

²⁶ <http://www.orbidcorp.com/>

²⁷ <http://www.packagent.com/>

²⁸ <http://www.rainingdata.com/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- Schreiner Prosecure

Schreiner Prosecure²⁹ offers several solutions for product authentication, among them KeySecure for worldwide tracing. With KeySecure, each item is identified as a unique specimen by a 15-digit encrypted, alphanumeric KeySecure Code printed as cleartext or barcode. Consumers and authorised personnel can verify the authenticity of products by online queries. Schreiner Prosecure also offers authentication based on security labels, including holograms, DNA identifiers, colour-shifting films, and laser film.

- SICPA

SICPATRACE is a solution provided by SICPA³⁰ for tagging, verifying, tracking and data management of products. SICPATRACE can be used to fight counterfeiting by determining where fake items in the supply chain are introduced. It can also help analyze the grey market by finding to which markets products are diverted to. The solution can either be used for online authentication or it can be integrated with back-end systems.

- Sun

Sun offers RFID solutions³¹ for different applications, one of which is authenticating pharmaceutical products. Two possibilities are used for this scenario. The first comprises authenticating a product by checking the EPC code on its RFID tag and comparing it with a repository of trusted codes. The other is a choice of electronic pedigree application provided by SupplyScape or RainingData.

- SupplyScape

SupplyScape³² E-Pedigree is a widely-adopted, ready-to-deploy electronic pedigree solution. It handles various requirements in a single system, including regulatory compliance and accommodating paper pedigrees in the system to handle legacy pedigrees. SupplyScape E-Pedigree integrates well with enterprise systems such as ERP and WMS which insures easier and more flexible adoption.

- Total Brand Security

Total Brand Security³³ (TBS) provides a toolbox of authentication technologies, mostly hardware-based, which can be layered onto the product thus providing several authentication mechanisms. These include unique packaging design, an infrared authentication system, security inks, holograms, and secure labels. One of the laser systems TBS offers was developed in the EU project NAGINELS (Non Aggressive Glass INternal Engraving Laser System). TBS also offers track and trace applications but they are not based on RFID because of its limited reliability in certain environments (e.g. metals and liquids). They use instead intelligent amorphous material threads the size of a hair that can carry a specific code. This code can then be read by taking measurements at a certain frequency from outside the package. The reading can be done through most materials including metals without the need for a line-of-sight. The main markets of TBS's products are the pharmaceuticals, electronics, spirits, perfumes and cosmetics industries.

²⁹ http://www.schreinergroup.de/wEnglisch/schreiner_prosecure/

³⁰ <http://www.sicpa.com/731/764.asp>

³¹ <http://www.sun.com/software/solutions/rfid/>

³² <http://www.supplyscape.com/>

³³ <http://www.totalbrandsecurity.com/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- Vardex Laser

Vardex Laser Corporation³⁴ created a laser marking system based on Variable Data Laser (VDL), a device that etches unique multi-layered security patterns onto a product's surface using pulsed laser light. The generated pattern can consist of 2D matrix, alpha-numeric and simple bar codes and can be combined with various images such as logos, date or production codes to form a compound codex. The result can be verified by a consumer and is machine-readable. By using different laser types, different material types can be marked. In addition to gelatine based products; glass, plastic and metals can also be marked reliably with permanent codes. Coding speed varies according to the type of material being marked and the amount/type of information applied to each piece. For simple codex, a single unit VDL System can produce over 500,000 marks per hour or 12,000,000 marks/24 h period.

- Verify Brand

Verify Brand³⁵ provides a platform for secure product serialisation, and real time, web-based product authentication, event management, tracking and reporting services. The first building block of the platform is Secure Code Control which is responsible of generating the unique codes (proprietary, EPCglobal, or imported from other sources) and printing them in various forms (barcodes, RFID, etc). The second building block is VeriSure, the module through which different parties can authenticate a particular product code. This can happen through a website or a call centre. Business rules defined by each brand owner dictate how the solution operates and responds to invalid code events. VeriSure can also create an electronic pedigree in real time. Finally, VeriTrack is a monitoring tool through which the entered and tracked codes and corresponding events can be logged and analyzed.

- Yottamark

The YottaMark³⁶ Authentication Platform is a solution based on encrypted codes that are applied to items or packaging units. The YottaMark security codes are generated on demand upon manufacturing or packaging and are encrypted, thus non-sequential and difficult to guess. Products marked with YottaMark security codes can be authenticated by different partners at different stages of the supply chain: manufacturers, brand protection personnel, law enforcement officials and even consumers can authenticate the products on the internet or using a camera phone, a hand-held scanner, or an SMS. The user receives a yes/no answer along with product and supply chain information. The YottaMark Authentication Platform keeps track of verified codes, including when and where codes are authenticated. Customised business rules evaluate authentications to detect suspicious patterns and duplicate codes.

3.3 Summary and Analysis of the Available Products

Although the focus of the previous section is on software-based systems such as track and trace and electronic pedigree based product authentication, solutions belonging to all five product authentication approaches distinguished in chapter 2 were identified. Below we give a summarizing recapitulation of solutions.

³⁴ <http://www.vardexlaser.com/>

³⁵ <http://www.verifybrand.com/>

³⁶ <http://www.yottamark.com/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Direct authentication based on product-inherent features. We gave examples of a few solutions based on direct authentication of product features:

- Fingerprint from AlpVision, based on comparing digital images of the product
- Authentix's authenticity test for spirits and drugs
- Ingenia's Laser Surface Authentication, based on a product's unique surface

From the information we collected, LSA looked particularly promising because of its apparent foolproofness, quick results returned, and ease of use.

Authentication based on difficult-to-reproduce features. The range of solutions presented here is wide-ranging:

- AuthentiFiber from Advanced Coding Systems, based on a magnetic feature
- Alpvision's Cryptoglyph, based on encrypted markings invisible to the human eye
- FractureCode's miniature codes, made of lines generated in random order
- Hyperlabel's suite, based on printing small infrared tags that encode information
- Microtaggant identification particles from Microtrace
- Orbid's 2DMI (2 Dimensional Mark Identification) marking technology
- Total Brand Security's (TBS) suite of technologies (inks, holograms, labels, etc)
- Variable Data Laser (VDL) laser etching from Vardex Laser Corporation

We conclude that there are numerous ways to be able to apply copy-protected features onto products and packages, with several solutions based on printing a unique pattern that is difficult to guess. In this case, the level of security is as good as the randomness used in generation, and the usefulness of the approach is determined by the ease of applying the verification process.

Verification of unique identifiers/track and trace data. We combine here the mechanisms of verification using unique identities and using track and trace data, since in many cases they coexist in the same products. Furthermore, there are only very few available solutions that employ intelligence to perform sophisticated plausibility checks that are based on the actual data. For these reasons, we lump various solutions, including ones that generate electronic pedigrees from the track and trace data, in the following group:

- Aegate's authentication system, uses RFID or barcodes in the pharmaceutical industry
- Authentix Serialized Authentication solution
- Axway's Synchrony ePedigree
- CounterFight's solution, uses serialisation with encrypted numbers
- DataFiber from Advanced Coding Systems
- Dintag corporation's distributed numbers and website authentication

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- PackAgent from Stora Enso and Trackway, identification and track and trace
- TigerLogic ePedigree solution from RainingData
- KeySecure from Schreiner Prosecure, unique identities based on encrypted keys
- Kezzler’s solution that identifies and tracks products based on kezzlercodes
- SICPATRACE from SICPA for analysing where fakes enter the supply chain
- SupplyScape E-Pedigree
- Yottamark Authentication Platform based on encrypted codes

Again, the range of solutions is wide and encompasses many vendors, which shows that the demand for product authentication solution is high, but at the same time that the degree of standardisation is low. Several solutions claim compliance with electronic pedigree regulations and EPCglobal standards, but in general the companies don’t provide a standard solution if not required to.

Cryptographic approaches. These are not used as often as other approaches, probably because of the high cost incurred and the complexity of setting up a cryptography infrastructure. The only solution of those we surveyed that indicated using cryptography is the one offered by Certicom, but even there it is only the tag identity which is encrypted and it is arguable if this is enough.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

4 State of Implementation of Technical Anti-Counterfeiting Measures in Relevant Industries

4.1 Introduction

In this chapter, the state-of-the-art regarding technical anti-counterfeiting measures in various industries relevant to the SToP project is described and analysed. We will cover the state of implementation in the pharmaceutical, aviation, luxury goods, and security document industries.

Our first goal is to describe which of the approaches and methods presented in this report are indeed used today. Clearly, only certain approaches and technologies are suitable for each industry, depending on characteristics of the industry, the products traded and the configuration of the supply chain. We will explain what these characteristics are and how they influence the adoption of anti-counterfeiting measures today. As these characteristics will prevail, they also set the boundaries for the design of the PVI. The following question guides the research presented in this chapter: What works in a certain industry and what does not and why so? Furthermore, contrasting the level of security that is achieved today with the desired state facilitates the identification of gaps that the PVI should fill.

The information presented in the following sections was gathered in multiple rounds of interviews with industry experts. The interviews were semi-structured and guided by a questionnaire that was distributed to the respondents beforehand. While some experts preferred to conduct face to face interviews, others provided written input first that was discussed in a subsequent face to face interview. Supplementary documents provided by the experts were utilised to complement the information gathered through the interviews.

Each of the following sections will describe the industry, product, and supply chain characteristics that impact the adoption of technical anti-counterfeiting measures, as well as characteristic problems of the industry with respect to counterfeiting, illegal product diversion, product safety and tampering. Our focus will be on describing which of the approaches and methods presented in chapter 2 are used in each industry and in which ways. We will also give an overview of the diffusion of anti-counterfeiting technologies and how often products are checked for genuineness during their lifecycle.

4.2 Pharmaceutical Industry

The pharmaceutical industry comprises research, development, production, marketing and distribution of drugs, most commonly in the context of healthcare. The industry is regulated and companies are subject to a variety of laws regarding the patenting, testing, producing and marketing of drugs. In 2006 global spending on prescription drugs reached \$602 billion³⁷.

Some characteristics of the products traded, the industry and the supply chain determine the suitability of product authentication approaches and technologies.

Relevant product characteristics:

³⁷ <http://www.wired.com/science/discoveries/news/2006/03/70508>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- worldwide availability of product
- vital importance to patient's health
- the safety of the patient is at risk as products are relatively easy to fake

Products in the pharmaceutical industry are of vital importance to the patient, so it is extremely important that an authentic product is used and not a fake. In developing countries the low purchasing power nurtures the demand for cheap vaccines and other regular medications. This mechanism provides a ground for counterfeited products. Several cases of fatalities have been reported because of the usage of counterfeited drugs.

Relevant industry characteristics:

- Highly regulated, with regulations differing across countries

The pharmaceutical industry is the most regulated industry due to patient safety. Regulations differ between countries, and within states in the USA, which puts further burden on manufacturers to comply with various regulations. In the USA, the Food & Drug Administration (FDA) only gives recommendations to the industry, but the actual regulations come from the state laws. For example, the state of California requires that an electronic pedigree for drugs is adopted by January 2009.

Supply chain characteristics:

- Usually the brand owner has limited control over what happens in the external supply chain.
- Drugs can be bought easily online

In the typical case, the manufacturers of pharmaceutical products do not have visibility of their supply chain beyond the first customer. Usually they buy point of sales information from customers (e.g. pharmacies) when they want to know where their products have gone and which supply chain routes they took.

We now present the types of problems faced by the pharmaceutical industry and the extent of the problems [LAG+06]. Counterfeit drugs have been detected in the past. The World Health Organization (WHO) describes counterfeit drugs as “deliberately and fraudulently mislabelled [drugs] with respect to identity and / or source. Counterfeiting can apply to all pharmaceutical products. Counterfeit products may include products with the correct ingredients or with the wrong ingredients, or with fake packaging.” The (WHO) estimates that approximately 10% of all drugs are counterfeit³⁸.

But why is it so easy to counterfeit drugs?

- Technology to produce most from labels to active pharmaceutical ingredients is widely available,
- Blockbuster “lifestyle” medicines that have created demand for illicit use,
- Globalization made distribution of counterfeited products intransparent,
- Internet provides easy access to potentially counterfeited products,

³⁸ <http://www.who.int/mediacentre/factsheets/fs275/en/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- An increase in a self-prescribing culture,
- Weak regulations in terms of law enforcement,
- Organised crime has become increasingly involved in counterfeiting as it becomes more profitable with lower risks than other drug trafficking.

The consequences of counterfeit drugs are manifold: (1) Patient's safety is at risk, (2) Social and economic consequences, (3) Producers face patent and copyright infringements (loss of revenue), (4) Governments have to deal with a loss of taxation revenues and undermining the National healthcare system, and (5) Considerable resources are required to combat counterfeiting.

In the remainder of this section, we present the authentication approaches used in the pharmaceutical industry.

Direct Authentication. This authentication method is based on inherent features of the drug product that can be verified in defined ways. Direct authentication is widely used within the pharmaceutical industry since it is the only way to reach a definite conclusion on the authenticity of a product. This is so because the inherent constituents of a drug cannot be easily copied or cloned the same way that most security features can be. Direct authentication can also be used as a proof of counterfeiting to indict charges on the counterfeiters. The authentication process is typically carried out on samples suspected to be counterfeited. The samples are collected and tested by the manufacturer.

An example of direct authentication is a fracture index analysis. Product verification through fracture index works in the following way: A pill is crushed and mixed with a special colour, the blend is then illuminated and a characteristic fracture index can be recorded. This approach is based on statistical methods and the analysis is so accurate that it can identify the production factory as output of the analysis. The time for the analysis is relatively low with this approach. Another method which is very widely used is performing a full chemical analysis by gas chromatography (GC). Professionals use GC to analyze the contents of chemical products because of its very accurate measures. The downside is a relatively long time for the analysis until the results are available.

The problem with direct authentication based on inherent features is that a full analysis is time consuming, as the suspect sample needs to be compared to an original sample from the same production run. It typically takes 2 to 3 weeks for the whole process from the identification of a suspect sample in the market to the conclusion regarding the authenticity of the product.

Authentication by means of a difficult to reproduce feature. Various different security features are used on drug packages to protect them against forgery. Such features are supposed to be hard to copy and the level of the protection provided is as good as the difficulty to forge these features or clone them. These features include security threads, digital watermarks, luminescent ink, IR ink, holograms, etc. These features can be applied in overt or covert ways, depending on the goals and strategy of the manufacturer. Some manufacturers prefer to use overt security features so that customers can make use of them. Other manufacturers prefer covert features, basically arguing that this strategy will cause more trouble for counterfeiters since they can't

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

copy something they do not even know it exists. Also, there are hybrid approaches that include a mixture of both. However, all features may be forged sooner or later.

Verification of unique identifiers. Unique identifiers such like batch numbers are easy to copy and can therefore not be used as appropriate authentication feature.

Unique identifiers on the sales pack level are used in the pharmaceutical industry mainly in pilot projects today. The vision behind this authentication method is to apply mass serialization on the sales packs in which each individual item has a unique number that identifies it. This number would then be used to make sure that this particular item is unique and that it was manufactured by the same entity that issues its unique identity. The item's unique identity can be used for further authentication as well as tracking the product through the supply chain thus enhancing its security level. Track and trace based verification is addressed in the next paragraph.

Today, pharmaceutical companies are building the experience to enable mass serialization on product packaging. This is driven by the need for increased patient safety as well as by upcoming regulations. It is expected that 2D barcodes and/or RFID are used as the tools for mass serialization. The deciding factor will primarily be the maturity of the technologies, global standards, and the incremental cost per package incurred.

Some examples of projects that use unique identifiers on the item level:

- Some manufacturers have limited pilots in place in the US market, where item level tagging of these two products is used. The program uses RFID technology for tagging the products which were probably chosen because they were susceptible to counterfeiting or grey market trade.
- There are some mature systems that use unique identifiers but are rather used to avoid reimbursement fraud than to combat counterfeiting. An example of such a system is the Bollino system put in place by the Italian government. In this system a linear barcode is applied to sales packs. It employs a central information directory in which companies are enforced to report the produced serial product information.

The main challenge which companies that want to introduce mass serialization face is the business integration especially for generics at a relatively low incremental cost. The mass serialization technologies are getting cheaper but it will still be very expensive to serialize all products a company sells. The second challenge is business integration, starting from maintaining the speed of the production process and to integrate the required information within the current information and enterprise systems. For example, a unique serial number to be applied to a sales pack needs to be requested, its uniqueness needs to be ensured and applied to the product, and finally traced through the distribution process.

Plausibility checks of track and trace data. The underlying vision behind using track and trace data for anti-counterfeiting assumes that all supply chain partners share the location information of the items they process. An overarching application (GS1-IS) would use additional intelligence to judge if the route that a certain sales pack took makes it suspicious. This assumes that mass serialization is widely in place which is impeded by the challenges as outlined in the previous paragraph. Companies work in cross-industry pilots to make this vision a reality. Most companies work

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

today to prepare the basis for track and trace within their internal information infrastructure. This includes having a GS1-IS in place with available item level information. If companies can have at least their internal item information handled, they will only have to connect to the GS1-IS of other companies, so that cross-supply chain tracking could be enabled. In summary, some pharmaceutical companies invest today to enable track and trace implementations tomorrow.

Limitations of this method include the links between drug product, packaging material and serial number. Another challenge is the integration with the existing information systems and business processes. Finally, track and trace functionality assumes that supply chain partners share information to authenticate products. This is not common practice today.

As demonstrated in the discussion above, most of the authentication options are increasingly used within the industry to protect the patient. The assumption within the pharmaceutical industry is that all technical features including RFID tags may be, counterfeited and defeat the intended use. Hence, the measures against counterfeiting need to include a dynamic approach regarding the technical features as well as other measures like stricter enforcement of existing laws.

4.3 Aviation Industry

The aviation industry, more specifically the civil aviation industry consists of only five major manufacturers of civil transport aircrafts: Airbus (Europe), Boeing (United States), Bombardier (Canada), Embraer (Brazil), and Tupolev (Russia).

The aviation industry is one of the highest regulated industries in the world. As passenger safety is of top priority, aircraft manufacturers have to comply with many standards. One of the crucial aspects is the airworthiness of parts that are used to build an aircraft. The relevant characteristics of aircraft parts are:

- Aircraft parts are specified by the aircraft manufacturer.
- Aircraft parts can be very expensive.
- The refurbishment of aircraft parts can be very expensive, e.g. up to 700,000 USD for a landing gear.
- Charges for testing that a part does not harm an aircraft amount to 500,000 USD.
- The safety of an airline passenger is at risk when faked or manipulated and thus unauthorised parts are built into an aircraft.

The lifecycle of an aircraft is depicted in Figure 12. In the beginning, parts are manufactured by licensed suppliers and then shipped to the aircraft manufacturer that assembles the aircraft from these parts. Then the aircraft is delivered to the airline that ordered it. In certain intervals, the aircraft has to be maintained, repaired, and overhauled. At these points in time the aircraft can change hands, i.e. be sold to another party. The lifecycle of an aircraft ends when it is scrapped.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

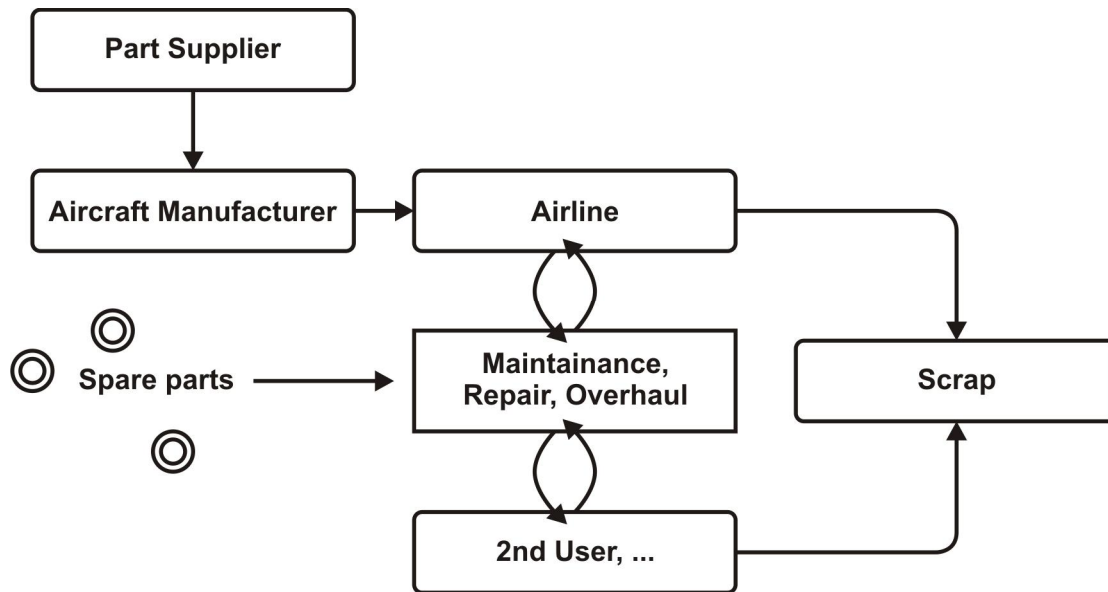


Figure 12: Lifecycle of an Aircraft

The aircraft manufacturer has control of the supply chain until it delivers the aircraft to the airline, as part suppliers have to be licensed and there are no intermediate partners within the supply chain. If the aircraft is later repaired, the aircraft manufacturer cannot influence which spare parts are used as replacements for original parts.

The Federal Aviation Administration (FAA), an agency of the United States Department of Transportation, recognises three categories for all parts:

- An approved part has been designed, produced, and maintained in accordance with FAA regulations and has documentation to prove it.
- An unapproved part is defined by the FAA as not meeting any one of the requirements for an approved part. This means that if there is any impropriety in the design, production, maintenance, or documentation of a part it may be unapproved and should not be used until substantiated. Examples are counterfeits, parts that have been received from unauthorised sources, as well as parts that have been maintained or repaired and returned to service by unauthorised persons or facilities [FAA95].
- A suspected unapproved part (SUP) is a part that is suspected of not meeting the requirements of an approved part. These parts may be deficient in quality or lack documentation to show where and how they were made.

According to the FAA, risks of unapproved parts are:

- Unapproved parts can jeopardise the safety of passengers and crew, e.g., one substandard bearing seal spacer could initiate a series of failures that result in the total internal failure of an engine during flight.
- Unapproved parts can undermine the structural and operational integrity of an aircraft causing increasing stress on all components over time.
- By using unapproved parts, however unintentionally, manufacturers, repair stations, operators and mechanics risk their reputation. If a failure occurs, they

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

are often automatically held responsible. Legal actions brought against the parties involved could damage or even disable their operations whether or not they are responsible.

- There are also economic implications. If an operator finds unapproved parts on their planes, they must pay the cost of removing the part and possibly delaying or cancelling flights. If a repair station or mechanic detects that they have used unapproved parts, the cost of recalls, parts failure and/or stoppage of production may result.

Currently, authentication of aircraft parts is entirely paper-based. A first measure to avoid unapproved parts is that aircraft manufacturers oblige part suppliers to fulfil certain requirements and comply with regulations. In individual cases though, manufacturers of high-quality counterfeit parts might get accidentally licensed. Accredited manufacturers have to provide design documents (including materials used, processes, and methods), test documents, and results of these tests for every part they deliver. They have to prove fit, form, and function within the DDP document (declaration on design and performance). Aircraft parts must also have a pedigree information document that allows for tracing and in case of defects for claiming damages. In addition to the paper documents, aircraft parts have to be equipped with barcodes, nameplates, and so called yellow tags required by the FAA that verify that they are genuine and have been manufactured in compliance with the specifications.

These documents and features are then inspected in detail. Corresponding parts are also tested again under real world conditions. As suppliers are liable for their parts, providing accurate documents is in their own interest. Furthermore, aircraft manufactures usually follow the same price policy worldwide to avoid parallel trade. Because of these regulations and policies it is nearly impossible that unapproved parts are used within new-built aircrafts.

Problems arise when spare parts come into play at the time when aircrafts are maintained, repaired, or overhauled as this is usually not up to aircraft manufacturers. At this point, the possibility that unapproved parts are built into aircrafts is much higher, for example because documents and features are not inspected carefully enough and suspicious parts therefore might not be detected. In most cases, these unapproved parts are not counterfeited but refurbished after they have been removed from scrapped or crashed airplanes. Another big problem is that the aforementioned documents are not copy protected and features can be easily removed from parts. If aircraft parts are optically perfect and documents are forged in a difficult to detect manner, it is nearly impossible to authenticate parts without investing a lot of time and money.

To further improve safety and protection against unapproved parts, the aviation industry is looking at RFID technology as a means to document the history and thus the whole lifecycle of parts. As Airbus and Boeing share up to 70 percent of their suppliers, the two rivals even started a cooperation to come up with a common RFID standard. The goal is to enforce suppliers to tag their parts by regulation. The SToP project will contribute to these efforts from a research perspective.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

4.4 Luxury Goods Industry

Luxury goods include as diverse product categories as wines and spirits, fashion and leather goods, perfumes and cosmetics, watches, and jewellery. Luxury brands signal to customers that they are buying a product that is superior in quality, durability, design or performance to comparable substitutes. Sold for a premium, luxury goods are not bought out of necessity. In some cases, they act as a status symbol and are bought to reflect the purchasing power of the buyer.

Several characteristics of luxury goods, the industry and the setup of the distribution channels play a significant role in determining the adoption of anti-counterfeiting technologies and the types of technologies employed. These characteristics are presented in more detail by work package 1, but as they are important for understanding the current state of implementation of technical countermeasures in the luxury goods industry, they will also be briefly introduced here.

Relevant product characteristics:

- Visual appearance of products is important
- Products may be extremely long-lived
- Most products do not threaten the safety of consumers

For all categories of luxury goods like clothing, handbags, or eyewear, aesthetics play an important role. It is thus not desirable that a security feature disfigures or spoils a product. The luxury goods industry is *selling dreams* and hints of product piracy issues are not easily compatible with this message. Security features are therefore often applied covertly.

Some luxury goods have a characteristically long lifespan. This holds true for hard luxury goods such as watches and jewellery, which are sometimes passed on from generation to generation as heirlooms. It is therefore desirable to employ security features that are as long-lived as the products themselves and that are capable of reliably authenticating products even after decades have passed since their manufacturing. In contrast to drugs and plane parts, and with some exceptions such as wines and spirits, perfumes or cosmetics, counterfeited or defunct luxury goods generally do not threaten the safety of consumers. Although counterfeiting poses a severe problem to the luxury goods industry in terms of lost revenues and brand value, the public, legal or external pressure to implement anti-counterfeiting measures is not as high as in the pharmaceutical and aerospace industry as consumer's lives are not immediately endangered.

Relevant industry characteristics:

- Luxury goods industry is not regulated
- High priced goods, in conjunction with high research and development, marketing costs
- Exclusiveness is a key argument for purchasing

Unlike the pharmaceutical or aerospace industry, the luxury goods industry is free from industry specific regulations. This is due to the fact that counterfeit luxury goods do not threaten consumer safety.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Luxury goods are high priced, the costs of products are being driven by production costs but also by characteristically high design, research and development, and marketing costs. As mentioned above, consumers are willing to pay a premium for luxury goods because they are perceived as status symbols and are of high quality and exclusive. While in the competitive luxury market costs are of importance, the price sensitivity of luxury goods clients and the relative cost impact of adding security features to luxury products is lower than in case of commodities, industrial or consumer goods. A key characteristic of most luxury goods is their exclusiveness and the existence of counterfeits threatens the core product offering.

Supply chain characteristics:

- Brand owner has a relatively high level of control, network of authorised dealers
- Legitimate internet sales remain limited

While some product categories are distributed through supply chains similar to those in place for consumer goods, others are distributed via selective distribution channels.

In selective distribution, brand owners can ensure that all sales are made in accordance with brand values and requirements. The usual message of brand owners is then that the only way for a client to be certain to purchase a genuine product is to buy it from a brand owner's boutique or an authorised dealer, either offline or online. Often sales of products by non-authorised retailers, on internet sites or auction platforms are primarily counterfeits and only secondarily diverted products or second-hand genuine products (example: LVMH suing eBay³⁹). In a selective distribution scenario, the licit supply chain is generally perceived as being free of counterfeits and relatively secure, although exceptions exist.

The primary problem of the luxury goods industry is counterfeiting, diversion being the secondary issue. Other threats mentioned in this report are of less importance. Both low and high-quality counterfeits can be found on the market, but high quality fakes (or non-perceptive counterfeits) are perceived as a more severe long term problem because customers can be more easily displeased and tricked into thinking they are buying a genuine product and the brand owner's revenues are more directly affected by the cannibalisation of legitimate sales.

Another peculiarity of the luxury industry is the prevalence of completely illicit supply chains. Although it is difficult to verify, counterfeit products are mostly manufactured in emerging countries and sold over the internet or auctioned off at electronic platforms such as eBay. Others are sold on flea markets or in small shops specializing in counterfeits. These products thus never even touch the licit supply chain. For brands that outsource their production, factory overruns are also an issue, with an increased risk if the production is outsourced to a remote and/or insufficiently monitored supplier. The strategy applied in the majority of cases by counterfeiters is to copy any visible product characteristic including any security feature in order to fool the customer. As many security features are applied covertly on luxury goods (and thus can only be checked by the brand owner), they are hardly a suitable tool for preventing customers from buying fake products. In the luxury goods industry, no cases of systematic reapplication of old security features are known.

³⁹ <http://www.lemonde.fr/web/article/0,1-0@2-651865,36-814854@51-809475,0.html>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

The extent of grey marketing heavily depends on the region of the world under consideration. While illicit trading and parallel imports are in itself a problem for the luxury goods industry, they are furthermore dangerous because they are misused by some counterfeiters to mix their counterfeited goods with genuine products. Customers can be tricked into believing that they buy a diverted product with a minor discount, but instead they receive a completely fake product.

There are no substantial cases of theft; relabelling is likewise not perceived as a challenge in the luxury goods industry. Tampering is an issue, for example gems in jewellery can be replaced or added to non-setted watchcases, but it is difficult to determine the scale of this problem. During transport and storage, integrity protection mechanisms suitable for the product in question are put in place. For expensive items which anyway require a secured environment, it seems that companies rely primarily on this trusted environment approach. As luxury goods are quite expensive, only people that can supply sufficient credentials have access to the goods. Signatures are used to confirm and to trace who was in the trusted environment and who handled the products. We will know describe the authentication approaches used in the industry.

Direct authentication. Although it is difficult to verify, to our knowledge, many if not most of luxury goods do not bear an artificial security feature, and direct authentication is widely used. The first defence line against counterfeiting of luxury goods consists in their detailed specification and high quality. Products are often designed in such a way that they are hard to copy because they bear special characteristics. By comparing a suspicious product with an original, counterfeit products can be identified. Alternatively, a photo of an original product or of a special product characteristic (pattern, colour, clip, zipper, stitching etc.) can be used for comparison (abundant examples of photos of these special characteristics can be found on eBay forums⁴⁰). Photos are often used by consumers, as they do not have access to original products. However, brand owners and manufacturers cannot provide the public with detailed information on how to identify genuine products, as this information could also be used by counterfeiters to improve the quality of fakes. Manual or automated photo recognition may also be employed by brand owners. Experts from the goods manufacturer are moreover skilled in telling counterfeits from originals and they might have access to technical specifications or sample original products for verification purposes. As some products might be very old and luxury goods come in small quantities and many varieties, it can be difficult to find a sample product or even a proper specialist. Even if this is not a problem, the entire process of sending the suspicious product to the right expert and waiting for a conclusive answer is time-consuming and costly.

Further characteristics of certain luxury goods that can be exploited for direct authentication include the composition of metals (e.g., gold, titanium), the formula and chemical characteristics of perfumes or the specific weight of products. However, these characteristics will always apply to a group of objects and are therefore not unique. A unique identifier could be generated by analysing the structure of leather goods, but this method is not used today. Diamonds and gems are characterised by a set of features like clarity grade, colour grade, angle etc. The combination of these

⁴⁰ http://cgi3.ebay.com/ws/eBayISAPI.dll?ViewUserPage&userid=handbag_authentication_resources

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

characteristics yields an identity that is not unique, but not very widespread either and can thus be used for authenticating jewellery.

Checking these characteristics for establishing the authenticity of products is time consuming, costly, and requires special equipment. For some product types, some companies record selected characteristics that suited for authenticating products and can therefore potentially be used for detecting counterfeits. If these characteristics were stored in a shared database, this would enable a more systematic and partially automated check of luxury goods.

Authentication by means of a hard to reproduce feature. It is estimated that the use of artificial security features in luxury goods remains limited. Depending on the product type, the feature is either applied directly to the product, to the label, or to the packaging. Entry-level products are supposedly easier to produce and thus also easier to counterfeit with a good look-alike quality. It is expected that those entry-level and volume products, because they are at higher risk of being counterfeited, are more likely to be equipped with security features.

It also needs to be taken into account that the visual appeal of the products must not be impacted. Printing visual marks – (e.g., a CDP or a 2D barcode) – directly on a product would be aesthetically unacceptable. Therefore, if a security feature is added, it is in most cases covert or even forensic. The security features employed are as diverse as the types of luxury goods, but optical features are quite commonly added to the packaging or the labels, for example micro engravings, holograms or printing with ink that is only visible in ultraviolet light. The existence of covert features is not made public, because counterfeiters shall not be encouraged to copy them. At the same time, this makes it impossible for costumers to distinguish between genuine and faked products.

The wider adoption of security features in the luxury goods industry is hindered by the difficulty to evaluate the commercially available products. It is hard to tell how secure these features really are and how long it will take counterfeiters to forge them. Moreover, the market for security features is heavily fragmented; many small technology providers offer products, all claiming theirs to be the most secure and impossible to clone.

A peculiarity of the luxury industry is the issuing of paper certificates to enable the authentication of certain product categories, (e.g., watches). This was made possible because the assignment of serial or limited series numbers to products has a long tradition for some luxury product categories. Historically, serial numbers have been put on several categories of products: some carry serial numbers by default, some only in case special limited series are manufactured. Serial numbers underline the limited supply and exclusiveness of products, but their main purpose was to keep track of the many varieties of products and to enable a correct servicing. The serial number will appear on the certificate, thus ensuring a binding between the product and the piece of paper. Some certificates are protected against copying with one or multiple security features.

Verification of unique identifiers. Serial numbers are quite common for certain categories of luxury goods. In this case, a brand owner can check the validity of the unique identifier and the compatibility with the numbering scheme to classify some products as counterfeits. This identification feature is not a full proof method, because

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

unless it is otherwise secured, the serial number can also be duplicated. In some instances the numbering is sequential and counterfeiters could guess series of valid numbers. It is more difficult when the numbering allocation is random.

Plausibility checks of track and trace data. Unlike in many other industries, item level tracking is already a reality for some categories of luxury goods. Moreover, a general trend towards capturing more and more item level tracking data can be observed in the luxury goods industry. Although serial numbers could be used for tracking, they are not always suited for this purpose as they might be engraved, printed, or generally hard to read. Therefore, tracking will usually be based on a visual data carrier that is easier to capture. When item level tracking is realised by a company, key logistic events are captured and stored in a single location, e.g., in a database that is under the control of the brand owner. When the brand owner does not control the entire supply chain of its products, the tracking might only partially cover the supply chain. The large-scale sharing of data between supply chain partners is generally perceived as difficult.

To our knowledge, track and trace data remains within brand owner’s boundaries and is not provided by brand owners for systematic plausibility checks by third parties such as retailers or customs. Secure object authentication is not used in the industry.

It is estimated that the usage of the above mentioned authentication features remains limited either with respect to the number of products covered or in its deployment all along the supply chain. Direct authentication likely remains for many products the only way of detecting counterfeits. For products that bear security marks, those applied are often covert. The best way to ensure that the product is authentic is to buy it via recognised or authorised retailers and boutiques. For most brand owners, the process of detecting counterfeits is slow, costly, and cumbersome.

Due the diversity of luxury product categories, there is not one approach that covers all products and is at the same time secure over a long time. It is also understood that with time all security features will be broken. There is a need for additional research that SToP should tackle and that should lead to a framework of approaches that cater to product and security technologies diversity and future evolutions. This framework should also support better collaboration between all involved parties (customs, retailers and possibly customers) without compromising the system security.

4.5 Security Document Industry

The security document industry is characterised by companies printing a broad range of documents that are potentially counterfeited or tampered. These include banknotes, visa and ID documents like identification cards or passports. Many of the documents are governmental documents. Accordingly, many states – for example the USA, France and Australia – have so called state printers. State printers are state-run companies producing security documents required by the state. The German Bundesdruckerei (BDR) used to be such a state printer, but was privatised in 2000. They provide a broad range of high security technologies, especially in the area of printing identification documents and value printing (e.g. EURO banknotes).

The domain of security documents is different from industries that aim at protecting classical industry products against counterfeiting or tampering, as done for example in the luxury goods industry. While in these industries the security efforts are characterised by economical constraints, i.e. the costs for the security feature itself,

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

costs of integration into the manufacturing process of the product and the costs of providing adequate verification infrastructures, within the security printing domain, all methods used are aimed at providing maximum security. Nevertheless, methods used within the area of high security technologies are not excluded from being used for product and trademark protection, as it is done using RFID for preventing counterfeiting of industry products.

Authentication by means of hard to reproduce features. The term authentication denotes, within the value printing industry, the unique assignment of a document to its manufacturer or publisher. This is achieved by the printing companies by including an adequate amount of security features into the documents. Examples for security features include watermarks and holograms, but also RFID tags or barcodes.

The security features are not used to authenticate products as defined above, but also to prevent forgery of the documents, for example through the assignment of passports of visa to other persons than they were originally issued to. In order to avoid tampering of security documents, a commonly used practice is the so called individualisation or personalisation of security features. This means, the security features include data about the content of the document. This individualisation can be coded in a way that it is not visible to somebody not knowing the code and the type of data being stored. In the case of a passport, this may be realised by storing data about the physical attributes of the person the passport belongs to in some security feature. Another way to avoid tampering of documents is the connection of security features. This means, a certain security feature has an attribute that must be combined with an attribute of another security feature, if the product is supposed to be considered genuine.

The level of security of a certain security feature is considered within the industry to be determined by the degree of information that is publicly available about the used technology, the technological capabilities of the feature, the availability of the used technology and to a large extent by the costs for the use of the feature. The last is based on the fact that no counterfeiter will copy a technology that costs him more than he benefits from it. This equation is fairly easy to solve for banknotes, because the value of the document is obvious, but for passports and other ID documents, the value that the document has for a counterfeiter is hard to estimate. Due to this fact, the investment in security features for identification products is higher than in banknotes. This fact also distinguishes the security document industry from other industries fighting counterfeiting.

Within the field of document security, it is distinguished between security and safety of security features of documents. While the term security denotes the protection that a security feature offers against tampering or counterfeiting of a document, the term safety refers to the durability of the feature. A document that has long time validity must be insusceptible to salt water, bending, ultraviolet radiation and many more external influences. Although the safety of a security feature plays an important role for the security document industry, this is not necessarily an issue for potential counterfeiters.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

Within the security document industry, security features are categorised in three levels:

- Level 1: These are security features that can be checked visually without any special equipment and special knowledge of the investigating person.
- Level 2: These are security features that need simple auxiliary means and according knowledge in order to authenticate a document.
- Level 3: These are technically based security features that can only be evaluated by means of special devices.

For the authentication of security features of documents, the Bundesdruckerei has an own device called VISIOTEC [BDR07], that checks the security features of passports. It is mainly used by customs and public authorities to verify the existence and integrity of the security features, read out the data and perform an integrity check.

Track and trace-based product authentication. The documents printed within the security documents industry require a strong consideration of the privacy of the person owning or carrying the document. This is conflictive with the approach of tracking documents and, based on the tracked data, making assumptions in regards to whether the product is genuine or not.

In case of the German passport, the problem of traceability has been solved by ensuring that the RFID tag contained in the passport provides a different identification number every time it is activated. Only after the transmission of a key that is read optically from a barcode integrated in the passport, communication between a reader and the tag can take place. Together with the conventional data stored on the tag, a signature (created at the personalization cycle by the authority) is stored that ensures that the data was not tampered.

As all data regarding personal documents is stored centrally at the Bundesdruckerei, the data transport as well as the storage of the data is encrypted and strictly secured. After the personalization process all data is deleted.

4.6 Analysis

In this section, the findings of the chapter discussing the state of implementation of technical anti-counterfeiting measures within the pharmaceutical, aviation, luxury goods and security documents industry are summarised. Furthermore, the particular problems of each industry and their overlaps and distinctions will be presented. An overview of the state of implementation of anti-counterfeiting measures is provided in Table 4.

Counterfeiting is clearly perceived as the primary problem across all industries, which was to be expected given the scope of the SToP project. However, product diversion and tampering are likely seen as problems that have to be addressed. Product integrity problems and industry-specific as well as general requirements will be presented in greater detail in deliverable 1.2. Except for the luxury goods industry, all industries examined are highly regulated and ensuring the safety of consumers is a recurring topic. This explains the high demand for anti-counterfeiting products in these industries, particularly as it can be expected that legislative actions will be taken in the future, therefore companies need to prepare and consider their options. Product and

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

supply chain characteristics are very diverse across the industries, hinting at the need for industry specific anti-counterfeiting concepts.

The authentication approaches that are used today in each industry are also presented in Table 4. Most notably, direct authentication and authentication based on hard to reproduce features prevail. Approaches based on mass serialisation are starting to emerge and are being tested or evaluated by some enterprises. Secure object authentication, being still a research topic, is not yet being considered.

The lack of standards, the lack of flexible infrastructures that are able to adapt to different products and environments and the lack of security features and authentication methods that are proven to be highly reliable and long time resistant against attacks are perceived as adoption barriers for more sophisticated authentication methods than those employed today. These issues, that we started to explore in this report, will be tackled by the SToP project, thus providing industries with research results tailored to their needs.

Industry Feature	Pharmaceutical	Aviation	Luxury Goods	Security Documents
Industry Characteristics	<ul style="list-style-type: none"> Highly regulated Consumer safety crucial 	<ul style="list-style-type: none"> Highly regulated Passenger safety crucial 	<ul style="list-style-type: none"> Not regulated Consumer safety usually not at risk High priced goods 	<ul style="list-style-type: none"> Highly regulated Consumer safety not at risk Security primary goal
Product Characteristics	<ul style="list-style-type: none"> High importance of product availability 	<ul style="list-style-type: none"> Aircraft parts specified by aircraft manufacturer Expensive to be manufactured, refurbished and tested 	<ul style="list-style-type: none"> Visual appearance important Durability may be important Do not threaten safety of consumers (usually) 	<ul style="list-style-type: none"> Value of products partly hard to estimate (e.g. passport) Durability important
Supply Chain Characteristics	<ul style="list-style-type: none"> Limited influence of the brand owner Counterfeits online available 	<ul style="list-style-type: none"> SC controlled by aircraft manufacturer till MOL phase Maintenance not supervised 	<ul style="list-style-type: none"> Often controlled, selective distribution Counterfeits available online 	<ul style="list-style-type: none"> No control
Product Integrity Problems	<ul style="list-style-type: none"> Counterfeiting Parallel Trade 	<ul style="list-style-type: none"> Counterfeiting Tampering Parallel Trade Second hand products 	<ul style="list-style-type: none"> Counterfeiting Parallel Trade 	<ul style="list-style-type: none"> Counterfeiting Tampering
Authentication Approaches and Methods Used				
<i>Direct Authentication</i>	Widely used	Rather not used	Widely used	Used
<i>Copy Protected Feature</i>	Widely used	Used	Sometimes used	Widely used
<i>Verification of unique identifiers</i>	Used on batch-level, item-level planned	Used	Sometimes used on batch-level	Widely Used

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

<i>Track and Trace</i>	Pilots implemented	Used	Some products on item level, no plausibility checks	Not relevant
<i>Secure Object Authentication</i>	Envisaged		Not used	Widely used
Main Technologies Used	<ul style="list-style-type: none"> • Chemical Procedures • Overt/covert copy protected features 	<ul style="list-style-type: none"> • Pedigree documents • Barcodes • Proprietary “yellow tags” 	<ul style="list-style-type: none"> • Comparison with photos/specifications • Certificates • Serial numbers 	<ul style="list-style-type: none"> • Broad range of copy protected features • RFID
General Adoption of Technical Anti Counterfeiting Measures	Only direct authentication commonly used	Implementation of pedigree documents, but these are frequently not inspected thoroughly	Direct authentication and some security features, lack of standards and framework to foster adoption	Security has always been a primary topic within the industry and is widely adopted

Table 4: State of Implementation in Relevant Industries

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

5 Conclusion

This report gave a survey of existing authentication technologies in three different dimensions: (1) authentication approaches and technologies, (2) example commercial products that employ them, and (3) the application of these techniques in different industries.

In the first part, we surveyed the different product authentication approaches and technologies and described their strengths and weaknesses. We grouped the available techniques into the following distinct but related categories:

- Direct authentication based on product inherent features, such as a surface structure that a counterfeiter cannot reproduce
- Approaches that use security features that are supposed to be difficult to reproduce, such as watermarks, holograms, secure labels, and taggants
- Verification of unique identifiers which assumes that the manufacturers assign a unique number to each item moving in the supply chain.
- Plausibility checks of track and trace data, which aim at determining if a product is authentic or not (or estimate a probability of authenticity) based on the history of a product and the locations at which it was observed.
- Secure object authentication using lightweight approaches, and challenge-response or similar protocols based on cryptography.

We also presented several concepts complementing product authentication, including copy protection of tags, methods for enforcing the binding between a tag and a product, tamper detection mechanisms, and product status checks. Furthermore, potential problems such as privacy protection and network dependability issues were addressed.

In the second part of the report, we looked at the state-of-the-art in product authentication from a different dimension, namely that of the commercial implementations. We showed, by describing sample products that are commercially available, which methods are practically used for product authentication. We described the functionality of different products and why some products perform better or not at all in certain environments. For example, a product that uses a magnetic signature for authentication works well with liquids and most metals, as opposed to RFID, but because of its magnetic nature fails with ferromagnetic metals. We grouped the products as per the categories described above and showed that certain approaches, such as the validation of unique identifiers, are implemented in many products, but other approaches, such as plausibility checks or cryptography, are not used in many products, as these approaches are still a research topic or in the stage of first prototypes.

The third and last part of the report looked at an aspect which is crucial to our work within the SToP project and finding concepts for anti-counterfeiting. This aspect is the difference among the various industries affected by counterfeiting. We investigated here, by desk research and interviews with our project partners, the nature of counterfeiting in different industries and the measures taken to counter it. We focused on the particularities of each industry (including the products themselves and the

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

supply chain) that need to be taken into account when determining how counterfeiting can be fought efficiently in each industry. For example, different industries have different motives to fight counterfeiting, varying from patient safety in pharmaceuticals and aerospace to brand image and lost revenues in luxury goods. Because of these differences, the speed of adopting technical anti-counterfeiting measures in certain industries, such as pharmaceuticals and aerospace, is higher than in others. We also presented the authentication approaches and technologies used in different industries. By comparing the state of implementation across industries, it became once more evident that different industries have different needs and requirements, which will shape the authentication infrastructure to be developed by the SToP project.

In conclusion, we affirm that the broad knowledge we collected about anti-counterfeiting mechanisms and products is valuable and will be used to shape up a flexible and easy-to-adopt anti-counterfeiting infrastructure that takes into consideration the needs of different industries.

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

References

- [AK96] ANDERSON, Ross ; KUHN, Markus: Tamper Resistance – a Cautionary Note. In: *Proceedings of the 2nd USENIX Workshop on Electronic Commerce*, 1996. – http://www.usenix.org/publications/library/proceedings/ec96/full_papers/kuhn/kuhn.ps
- [AO05] AVOINE, Gildas ; OECHSLIN, Philippe: RFID Traceability: A Multilayer Problem. In: *Financial Cryptography and Data Security* Vol. 3570, Springer-Verlag, 2005 (LNCS), pp. 125–140
- [ATM06] ATMEL: *Standard Read/Write Crypto Identification IC – e5561*. http://www.atmel.com/dyn/resources/prod_documents/doc4699.pdf. Version: 2006
- [Avo07] AVOINE, Gildas: *Bibliography on Security and Privacy in RFID Systems*. <http://lasecwww.epfl.ch/gavoine/download/bib/bibliography-rfid.pdf>. Version: May 2007
- [BDR07] BDR (BUNDESDRUCKEREI): Verifizierung – Die VISIOTEC Lösungen. Version: 2007. http://www.bundesdruckerei.com/de/support/download/visotec_d.pdf. 2007. – Technical Report
- [BGK+06] BATINA, Lejla ; GUAJARDO, Jorge ; KERINS, Tim ; MENTENS, Nele ; TUYLS, Pim ; VERBAUWHEDE, Ingrid: *An Elliptic Curve Processor Suitable For RFID Tags*. <http://eprint.iacr.org/2006/227.pdf>. Version: 2006. – Cryptology ePrint Archive: Report 2006/227
- [BGKR06] BEIER, Steve ; GRANDISON, Tyrone ; KAILING, Karin ; RANTZAU, Ralf: Discovery Services – Enabling RFID Traceability in EPCglobal Networks. In: *Proceedings of the 13th International Conference on Management of Data*, 2006. – <http://www.almaden.ibm.com/cs/projects/iis/hdb/Publications/papers/comad2006.pdf>
- [Bro01a] BROCK, David L.: The Electronic Product Code (EPC) / Auto-ID Center, Massachusetts Institute of Technology, USA. Version: 2001. <http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH-002.pdf>. 2001 (MIT-AUTOID-WH-002). – Technical Report
- [Bro01b] BROCK, David L.: Integrating the Electronic Product Code (EPC) and the Global Trade Item Number (GTIN) / Auto-ID Center, Massachusetts Institute of Technology, USA. 2001 (MIT-AUTOID-WH-004). – Technical Report
- [BSI04] BSI (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK): Security Aspects and Prospective Applications of RFID Systems / Federal Office for Information Security. Version: 2004. http://www.bsi.bund.de/fachthem/rfid/RIKCHA_englisch_layout.pdf. 2004. – Technical Report
- [CKS07] CHEUNG, Alvin ; KAILING, Karin ; SCHÖNAUER, Stefan: Theseos: A Query Engine for Traceability across Sovereign, Distributed RFID Databases. In: *Proceedings of the 23rd International Conference on Data Engineering*, 2007
- [CLB06] CHATMON, Christy ; LE, Tri van ; BURMESTER, Mike: Secure Anonymous RFID Authentication Protocols / Florida State University, Department of Computer Science. Version: 2006. <http://www.cs.fsu.edu/research/reports/TR-060112.pdf>. 2006 (TR-060112). – Technical Report
- [CLL05] CHOI, Eun Y. ; LEE, Su M. ; LEE, Dong H.: Efficient RFID Authentication Protocol for Ubiquitous Computing Environment. In: ENOKIDO, Tomoya (Hrsg.): *Embedded and Ubiquitous Computing – EUC 2005 Workshops* Vol. 3823, Springer-Verlag, 2005 (LNCS), pp. 945–954
- [Col04] COLLINS, Jonathan: African Beef Gets Tracked. In: *RFID Journal* (2004). <http://www.rfidjournal.com/article/articleprint/1281/-1/1/>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- [DFJ07] DEFEND, Benessa ; FU, Kevin ; JUELS, Ari: Cryptanalysis of Two Lightweight RFID Authentication Schemes. In: *Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*. Washington, DC : IEEE Computer Society, 2007, pp. 211–216
- [Dim05] DIMITRIOU, Tassos: A Lightweight RFID Protocol to protect against Traceability and Cloning attacks. In: *Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks*. Washington, DC : IEEE Computer Society, 2005, pp. 59–66
- [Dim06] DIMITRIOU, T.: A Secure and Efficient RFID Protocol that could make Big Brother (partially) Obsolete. In: *Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications*. Washington, DC : IEEE Computer Society, 2006, pp. 269–275
- [DMS07] DIEKMANN, Thomas ; MELSKI, Adam ; SCHUMANN, Matthias: Data-on-Network vs. Data-on-Tag: Managing Data in Complex RFID Environments. In: *Proceedings of the 40th Hawaii International Conference on System Sciences*. Washington, DC : IEEE Computer Society, 2007, 224a. – <http://csdl.computer.org/comp/proceedings/hicss/2007/2755/00/27550224a.pdf>
- [DPLK06] DUC, Dang N. ; PARK, Jaemin ; LEE, Hyunrok ; KIM, Kwangjo: Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning. In: *Proceedings of the 2006 Symposium on Cryptography and Information Security*. Hiroshima, Japan, January 2006
- [EHJ04] ENGBERG, Stephan J. ; HARNING, Morten B. ; JENSEN, Christian D.: Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience. In: *Proceedings of the 2nd Annual Conference on Privacy, Security and Trust*. New Brunswick, Canada, October 2004
- [EPC05a] EPCGLOBAL: *The Application Level Events (ALE) Specification, Version 1.0*. http://www.epcglobalinc.org/standards/Application_level_events_aLE_standard_version_1.0.pdf. Version: 2005
- [EPC05b] EPCGLOBAL: *EPC Radio-Frequency Identity Protocols – Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.0.9*. http://www.epcglobalinc.org/standards/Class_generation_uHF_air_interface_protocol_standard_version_1.0.9.pdf. Version: 2005
- [EPC05c] EPCGLOBAL: *The EPCglobal Architecture Framework*. http://www.epcglobalinc.org/standards/Final-epcglobal-architecture_20050701.pdf. Version: 2005
- [EPC05d] EPCGLOBAL: *Object Naming Service (ONS) Version 1.0*. http://www.epcglobalinc.org/standards/Object_naming_service_ons_standard_version_1.0.pdf. Version: 2005
- [EPC06a] EPCGLOBAL: *EPC Information Services (EPCIS) Version 1.0 Specification – Proposed Specification Version of 29 November 2006*. 2006
- [EPC06b] EPCGLOBAL: *EPCglobal Certificate Profile*. http://www.epcglobalinc.org/standards/EPCglobal_certificate_profile.pdf. Version: 2006
- [EPC06c] EPCGLOBAL: *EPCglobal Tag Data Standards Version 1.3*. http://www.epcglobalinc.org/standards/EPCglobal_tag_data_standard_tDS_version_1.1_revision_1.27.pdf. Version: 2006
- [EPC06d] EPCGLOBAL: *EPCglobal Tag Data Translation (TDT) 1.0*. http://www.epcglobalinc.org/standards/EPCglobal_tag_data_translation_tDT_standard_1.0.pdf. Version: 2006
- [EPC06e] EPCGLOBAL: *Reader Management 1.0*. http://www.epcglobalinc.org/standards/RM_ratified_standard_dec_2006.pdf. Version: 2006

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- [EPC06f] EPCGLOBAL: *Reader Protocol Standard, Version 1.1*. http://www.epcglobalinc.org/standards/Reader_protocol_standard.pdf. Version: 2006
- [EPC07] EPCGLOBAL: *Pedigree Ratified Standard Version 1.0*. http://www.epcglobalinc.org/standards/Ratified_drug_pedigree_standard_jan_2007.pdf. Version: 2007
- [FAA95] FAA: Suspected Unapproved Parts Program Plan / Federal Aviation Administration. Version: 1995. <http://www.faa.gov/aircraft/safety/programs/sups/media/supfn111.pdf>. 1995. – Technical Report
- [Fin06] FINKENZELLER, Klaus: *RFID Handbuch*. 4. Auflage. München Wien : Hanser Verlag, 2006
- [FWR05] FELDHOFFER, Martin ; WOLKERSTORFER, Johannes ; RIJMEN, Vincent: AES implementation on a grain of sand. In: *IEE Proceedings – Information Security*, 2005
- [GC06] GRASSO, Alfio R. ; COLE, Peter H.: Definition of Terms used by the Auto-ID Labs in the Anti-Counterfeiting White Paper Series / Auto-ID Lab, University of Adelaide, Australia. Version: 2006. <http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-HARDWARE-024.pdf>. 2006 (WP-HARDWARE-024). – Technical Report
- [GRS05] GILBERT, Henri ; ROBshaw, Matt ; SIBERT, Hervé: An Active Attack Against HB+ – A Provably Secure Lightweight Authentication Protocol. In: *IEE Electronics Letters* 41 (2005), No. 21, pp. 1169–1170
- [GXW+04] GAO, Xingxin ; XIANG, Zhe ; WANG, Hao ; SHEN, Jun ; HUANG, Jian ; SONG, Song: An approach to security and privacy of RFID system for supply chain. In: *Proceedings of the 2004 IEEE International Conference on E-Commerce Technology for Dynamic E-Business*, IEEE Computer Society, 2004, pp. 164–168
- [HB00] HOPPER, Nicholas ; BLUM, Manuel: A Secure Human-Computer Authentication Scheme / Carnegie Mellon University, School of Computer Science. Version: 2000. www.aladdin.cs.cmu.edu/papers/pdfs/y2001/manuel_blum.pdf. 2000 (CMU-CS-00-139). – Technical Report
- [HM04] HENRICI, Dirk ; MÜLLER, Paul: Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. In: *Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops*. Washington, DC : IEEE Computer Society, 2004
- [HMBM03] HARRISON, Mark ; MORAN, Humberto ; BRUSEY, James ; MCFARLANE, Duncan: PML Server Developments. Version: 2003. <http://www.autoidlabs.org/uploads/media/CAM-AUTOID-WH015.pdf>. 2003 (CAM-AUTOID-WH-015). – Technical Report
- [Hom05] HOMPEL, Michael ten: RFID ist eine Chance für den Standort. In: *METRO Group RFID Newsletter* (2005), April, No. 2, 6. http://www.future-store.org/servlet/PB/show/1004467/RFIDnet-Newsletter-02-2005-dt_05-04-20.pdf. – http://www.future-store.org/servlet/PB/show/1004467/RFIDnet-Newsletter-02-2005-dt_05-04-20.pdf
- [HS06] HARRISON, Mark ; SHAW, Andy: Electronic Pedigree and Authentication Issues for Aerospace Part Tracking / Auto-ID Lab, University of Cambridge, United Kingdom. Version: 2006. http://aero-id.org/mediawiki/img_auth.php/8/82/Aeroid-cam-001-pedigree.pdf. 2006 (AEROID-CAM-001). – Technical Report
- [HVRZ07] HUANG, Dijiang ; VERMA, Mayank ; RAMACHANDRAN, Archana ; ZHOU, Zhibin: A Distributed ePedigree Architecture. In: *Proceedings of the 11th International Workshop on Future Trends of Distributed Computing Systems*, 2007. – <http://snac.eas.asu.edu/snac/document/A>

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- [IBM07] IBM: *Enabling RFID Traceability in EPCglobal Networks*. http://dl.alphaworks.ibm.com/technologies/theseos/RFID_traceability.pdf. Version: 2007
- [Ina07] INABA, Tatsuya: EPC System for Safe & Secure Supply Chain and How it is applied. Version: 2007. <http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-BIZAPP-026.pdf>. In: *EPC System for Safe and Secure Supply Chain and How it is Applied*. Springer-Verlag, 2007 (WP-BIZAPP-026)
- [Joh05] JOHNSTON, Roger G.: An Anti-Counterfeiting Strategy Using Numeric Tokens. In: *International Journal of Pharmaceutical Medicine* 19 (2005), No. 3, 163-171. http://www.verifybrand.com/pdf/Drug_anti-Counterfeiting_2004.pdf
- [JP03] JUELS, Ari ; PAPPU, Ravikanth: Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In: *Financial Cryptography* Vol. 2742, Springer-Verlag, 2003 (LNCS)
- [JRS03] JUELS, Ari ; RIVEST, Ronald ; SZYDLO, Michael: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In: *Proceedings of the 10th ACM Conference on Computer and Communications Security*. New York, NY : ACM Press, 2003, pp. 103–111
- [Jue04] JUELS, Ari: Minimalist Cryptography for Low-Cost RFID Tags. In: *Security in Communication Networks*, Springer-Verlag, 2004 (LNCS 3352)
- [Jue05] JUELS, Ari: Strengthening EPC Tags Against Cloning. In: *Proceedings of the 4th ACM Workshop on Wireless Security*. New York : ACM Press, 2005, pp. 67–76
- [Jue06] JUELS, Ari: RFID Security and Privacy: A Research Survey. In: *IEEE Journal on Selected Areas in Communications* 24 (2006), February, No. 2, pp. 381–394
- [JW05] JUELS, Ari ; WEIS, Stephen A.: Authenticating Pervasive Devices with Human Protocols. In: *Advances in Cryptology – CRYPTO 2005* Vol. 3126, Springer-Verlag, 2005 (LNCS)
- [KM05] KARJOTH, Günter ; MOSKOWITZ, Paul: Disabling RFID Tags with Visible Confirmation: Clipped Tags are Silenced. In: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. New York : ACM Press, 2005, pp. 27–30
- [KS06] KATZ, Jonathan ; SHIN, Ji S.: Parallel and Concurrent Security of the HB and HB+ Protocols. In: *Advances in Cryptology – EUROCRYPT 2006* Vol. 4004, Springer-Verlag, 2006 (LNCS)
- [KSCB03] KOH, Robin ; SCHUSTER, Edmund W. ; CHACKRABARTI, Indy ; BELLMAN, Attilio: Securing the Pharmaceutical Supply Chain / Auto-ID Center, Massachusetts Institute of Technology, USA. Version: 2003. <http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH021.pdf>. 2003 (MIT-AUTOID-WH-021). – Technical Report
- [LAK06] LEE, Sangshin ; ASANO, Tomoyuki ; KIM, Kwangjo: RFID Mutual Authentication Scheme based on Synchronized Secret Information. In: *Proceedings of the 2006 Symposium on Cryptography and Information Security*. Hiroshima, Japan, January 2006
- [LAKR+06] LEHTONEN, Mikko ; AL-KASSAB, Jasser ; REISCHACH, Felix G. ; KASTEN, Oliver ; MICHAHELLES, Florian: Problem-Analysis Report on Counterfeiting and Illicit Trade. 2006 (BRIDGE Deliverable 5.1). – Technical Report
- [LHLL05] LEE, Su M. ; HWANG, Young J. ; LEE, Dong H. ; LIM, Jong I.: Efficient Authentication for Low-Cost RFID Systems. In: GERVASI, Osvaldo (Hrsg.): *Computational Science and Its Applications – ICCSA 2005* Vol. 3480, Springer-Verlag, 2005 (LNCS), pp. 619–627
- [Lin07] LINGLE, Rick: RPC Provides Protection and Security. In: *Packaging World* (2007). <http://www.packworld.com/view-22870>
- [LLG+04] LEE, Jae W. ; LIM, Daihyun ; GASSEND, Blaise ; SUH, G. E. ; DIJK, Marten van ; DEVADAS, Srin: A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications. In: *Proceedings of the 2004 Symposium on VLSI Circuits*. Washington : IEEE Computer Society, 2004, pp. 176–179
- [LM07] LANGHEINRICH, Marc; MARTI, Remo: Practical Minimalist Cryptography for RFID Privacy. In: *IEEE Systems Journal, Special Issue on RFID Technology*, December 2007

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- [LSMF06] LEHTONEN, Mikko ; STAAKE, Thorsten ; MICHAHELLES, Florian ; FLEISCH, Elgar: From Identification to Authentication - A Review of RFID Product Authentication Techniques / Auto-ID Lab, ETH Zurich/St.Gallen, Switzerland. Version: 2006. <http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-BIZAPP-029.pdf>. 2006 (WP-BIZAPP-029). – Technical Report
- [LW07] LI, Tiejian ; WANG, Guilin: Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols. In: *Proceedings of the 22nd IFIP TC-11 International Information Security Conference*, 2007
- [MOV96] MENEZES, Alfred J. ; OORSCHOT, Paul C. ; VANSTONE, Scott A.: *Handbook of Applied Cryptography*. CRC Press, 1996
- [MP05] MALLINSON, Hugo ; PARLIKAD, Ajith: *RFID-based Product Data Management*. http://www.bestshore.net/library/product_data_mng.pdf. Version: August 2005
- [MSW05] MOLNAR, David ; SOPPERA, Andrea ; WAGNER, David: *A scalable, delegatable, pseudonym protocol enabling ownership transfer of RFID tags*. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005
- [MW04] MOLNAR, David ; WAGNER, David: Privacy and Security in Library RFID Issues, Practices, and Architectures. In: *Proceedings of the 11th ACM Conference on Computer and Communications Security*. New York : ACM Press, 2004, pp. 210–219
- [NSF06] NOCHTA, Zoltán ; STAAKE, Thorsten ; FLEISCH, Elgar: Product Specific Security Features Based on RFID Technology. In: *Proceedings of the International Symposium on Applications and the Internet Workshops*, IEEE Computer Society, 2006. – <http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-BIZAPP-028.pdf>
- [O’C05] O’CONNOR, Mary C.: Bar Coding for Item Tracking. In: *RFID Journal* (2005). <http://www.rfidjournal.com/article/articleview/1309/1/1/>
- [O’C07] O’CONNOR, Mary C.: Packaging Maker Offering Tamper-Evident RFID Film. In: *RFID Journal* (2007). <http://www.rfidjournal.com/article/articleview/2959/>
- [OSK03] OHKUBO, Miyako ; SUZUKI, Koutarou ; KINOSHITA, Shingo: Cryptographic Approach to Privacy-Friendly Tags. In: *RFID Privacy Workshop*, 2003
- [PAK99] PETITCOLAS, Fabien ; ANDERSON, Ross ; KUHN, Markus: Information Hiding – A Survey. In: *Proceedings of the IEEE, special issue on protection of multimedia content* 87 (1999), No. 7, pp. 1062–1078. <http://dx.doi.org/10.1109/5.771065>. – DOI 10.1109/5.771065
- [Pea05] PEARSON, Joseph: Securing the Pharmaceutical Supply Chain with RFID and Public-key infrastructure (PKI) Technologies / Texas Instruments Inc. Version: 2005. http://www.ti.com/rfid/docs/manuals/whtPapers/wp-RFID_and_pKI.pdf. 2005 (RFIDPH01). – Technical Report
- [Pea06] PEARSON, Joseph: RFID Tag Data Security Infrastructure: A Common Ground Approach for Pharmaceutical Supply Chain Safety / Texas Instruments. Version: 2006. http://www.ti.com/rfid/docs/manuals/whtPapers/wp-Tag_data_security_infrastructure.pdf. 2006 (RFIDHF02). – Technical Report
- [Pir06] PIRAMUTHU, Selwyn: HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication Title. In: *Proceedings of COLLECTeR Europe 2006*, 2006, 239-247
- [PSR04] PSR (PRODUCT SURETY CENTER): The Product Surety Working Group Initiative Final Report. Version: 2004. http://www.productsurety.org/documents/TheProductSuretyFinal_march04_vPublic.pdf. 2004. – Technical Report
- [PSR05] PSR (PRODUCT SURETY CENTER): Symposium on Risks in Supply Chains. 2005. – Technical Report

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 3.1		
Title	Report on relevant state-of-the-art research, existing technologies and products	Date	2007-11-08

- [RCT05] RIEBACK, Melanie ; CRISPO, Bruno ; TANENBAUM, Andrew: RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. In: *Information Security and Privacy* Vol. 3574, Springer-Verlag, 2005 (LNCS), 184-194
- [REC04] RANASINGHE, Damith C. ; ENGELS, Daniel W. ; COLE, Peter H.: Security and Privacy: Modest Proposals for Low-Cost RFID Systems. In: *Auto-ID Labs Research Workshop*. Zurich, Switzerland, September 2004
- [RFI04] RFID JOURNAL: RFID News Roundup. In: *RFID Journal* (2004)
- [RKKW05] RHEE, Keunwoo ; KWAK, Jin ; KIM, Seungjoo ; WON, Dongho: Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment. In: *Security in Pervasive Computing* Vol. 3450, Springer-Verlag, 2005 (LNCS), pp. 70–84
- [SAB07] SCHUSTER, Edmund W. ; ALLEN, Stuart J. ; BROCK, David L.: *Global RFID*. Berlin Heidelberg : Springer-Verlag, 2007
- [Sem07] SEMICONDUCTORS, NXP: *MIFARE contactless smart card ICs*. <http://www.nxp.com/products/identification/mifare/index.html>, April 2007
- [SMTF06] STAAKE, Thorsten ; MICHAELLES, Florian ; THIESSE, Frédéric ; FLEISCH, Elgar: *Anti-Counterfeiting Special Interest Group – Project Report*. June 2006
- [Sta02] STAJANO, Frank: *Security for Ubiquitous Computing*. John Wiley & Sons, 2002
- [STF05] STAAKE, Thorsten ; THIESSE, Frédéric ; FLEISCH, Elgar: Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting. In: *Proceedings of the 2005 ACM Symposium on Applied Computing*. New York : ACM Press, 2005, 1607-1612
- [TB06] TUYLS, Pim ; BATINA, Lejla: RFID-Tags for Anti-Counterfeiting. In: *Topics in Cryptology – CT-RSA 2006* Vol. 3860, Springer-Verlag, 2006 (LNCS), pp. 115–131
- [TRB03] TRB (TRANSPORTATION RESEARCH BOARD): *Cybersecurity of Freight Information Systems – A Scoping Study*. 2003 (274). – Technical Report
- [TSM01] THEDE, Anke ; SCHMIDT, Albrecht ; MERZ, Christian: Integration of Goods Delivery Supervision into E-commerce Supply Chain. In: *Electronic Commerce* Vol. 2232, Springer-Verlag, 2001 (LNCS)
- [Tsu06] TSUDIK, Gene: YA-TRAP: Yet another trivial RFID authentication protocol. In: *Proceedings of the 4th annual IEEE international conference on Pervasive Computing and Communications Workshops*. Washington : IEEE Computer Society, 2006, pp. 640–643
- [VB03] VAJDA, István ; BUTTYÁN, Levente: Lightweight Authentication Protocols for Low-Cost RFID Tags. In: *2nd Workshop on Security in Ubiquitous Computing*. Seattle, October 2003
- [Ver05] VERISIGN: Beyond Pedigree: The Role of Infrastructure in the Pharmaceutical Supply Chain. Version: 2005. <http://www.verisign.com/static/031078.pdf>. 2005. – Technical Report
- [WN02] Winsborough, W.H. and N. Li. Towards Practical Automated Trust Negotiation. in *Proceedings of the Third International Workshop on Policies for Distributed Systems and Networks*. 2002. Monterey, CA
- [WSRE03] WEIS, Stephen A. ; SARMA, Sanjay E. ; RIVEST, Ronald L. ; ENGELS, Daniel W.: Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems. In: *Security in Pervasive Computing* Vol. 2802, Springer-Verlag, 2003 (LNCS), pp. 201–212
- [YPL+05] YANG, Jeongkyu ; PARK, Jaemin ; LEE, Hyunrok ; REN, Kui ; KIM, Kwangjo: *Mutual Authentication Protocol for Low-cost RFID*. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005
- [ZK05] ZHANG, Xiaolan ; KING, Brian: Integrity Improvements to an RFID Privacy Protection Protocol for Anti-counterfeiting. In: *Information Security* Vol. 3650, Springer-Verlag, 2005 (LNCS), pp. 474–481