



Project IST-034144: SToP
Stop Tampering of Products

Deliverable 5.4

Final Application Guidelines for Companies of Different Size

Leading Partner: SAP

Security Classification: Public (PU)

September 2009

Version 1.0

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)	Harald Vogt (SAP) Mikko Lethonen (ETH) Felix von Reischach (SAP) Daniel Boos (ETH) Ali Dada (SAP) Jens Müller (SAP) Carsten Magerkurth (SAP) Nina Oertel (SAP)		
Responsible Author (Partner)	Harald Vogt (SAP)	E-mail	harald.vogt@sap.com
		Phone	+49 6227 7 52551

Version History

Version	Date	Description	Comments
0.9	09-07-15	Draft	
0.95	09-09-07	Completed version	Ready for review
0.96	09-09-11	Partner feedback integrated	
1.0	09-09-22	Final version	

Table of Contents

Project Details	I
Version History	I
Table of Contents	II
Table of Figures	III
Table of Tables.....	III
Executive Summary	1
1 Introduction	3
2 Background	4
2.1 The Business of Counterfeiting.....	4
2.2 Anti-Counterfeiting Approaches.....	6
2.3 Auto-ID, RFID and Ambient Intelligence.....	7
3 A Comprehensive Approach to Anti-Counterfeiting.....	8
3.1 What Kind of System?.....	8
3.2 Securing a Supply Chain	9
3.2.1 Addressing the Supply of Counterfeit Goods.....	10
3.2.2 Addressing the Counterfeiting of Serial Numbers.....	12
3.2.3 Addressing the Sales of Counterfeits	13
3.3 Business Process Set-Up	14
3.3.1 Production.....	14
3.3.2 Transport.....	15
3.3.3 Retail	16
3.3.4 Analytics.....	16
3.3.5 Incident Response	17
3.3.6 Protection of Intellectual Property	18
4 Implementation.....	20
4.1 Anti-Counterfeiting Measures	20
4.2 Feature Selection and Integration.....	21
4.3 Verification Infrastructure	24
4.3.1 Technical Infrastructure.....	24
4.3.2 Employee motivation and awareness	25
4.3.3 A System for Product Verification.....	26
4.3.4 Business System Integration.....	27
4.4 Usability.....	29
4.4.1 User Interface.....	29
4.4.2 Work Flow and Workplace Management.....	30
5 Conclusion.....	30
6 References	33

Table of Figures

Figure 1. Overview of the most important Auto-ID technologies	7
Figure 2: The Integrated process of securing a supply chain against counterfeits.....	11
Figure 3. Summary of existing approaches to fight product counterfeiting	21
Figure 4: RFID tag integration in a watch frame	22
Figure 5: Basic Components of the Technical Infrastructure	24
Figure 6: Reader devices	25
Figure 7: General architecture of a system for product verification	27
Figure 8: Business processes accessing product verification	28

Table of Tables

Table 1: Drivers and enablers of illicit trade	5
Table 2. Summary of intellectual property rights [9].....	19
Table 3: Criteria for technology selection	23

Executive Summary

The SToP project has investigated how features for product authentication could be intrinsically built into products and supply chain processes such that the reliable identification of counterfeit items becomes possible and the sources of these counterfeits could be tracked down. The project team has developed and evaluated mechanisms and prototypical tools to

- analyse the motivations and structures of counterfeiters,
- assess and calculate the impact of the presence of counterfeit items on businesses in various industries,
- protect supply chains by identifying and responding to the appearance of counterfeit items,
- integrate advanced RFID-based identification devices in products,
- analyse supply chains based on item-level event data, and
- integrate product authentication functionality in existing systems for business operations.

The detailed results of these activities are accessible in project reports, which are largely published on the project web site, www.stop-project.eu. Based on these results, we have assembled recommendations and guidelines on the application of comprehensive infrastructures for product authentication.

The guidelines and recommendations discussed in this deliverable take a holistic approach on the problem domain of counterfeiting and encompass fundamental considerations as well as technical, organisational, and implementation issues applied to different critical fields such as the security of the supply chain, the schemes for serialization of items or the sale of counterfeit items.

A strong focus is also on the appropriate security feature selection as a result of both the RFID and hardware related innovative research carried out in the project as well as because of the fundamental implications from the supply chain setup and the effects on the cost and benefit assessment of the solution.

It is however important to stress that the technical and financial issues of selecting the optimal set of security features alone does not guarantee an appropriate protection from fraud and tampered products. A holistic approach is vital for the efficacy of an anti-counterfeiting solution, since a disregard of certain perspectives might lead to corresponding activities on the counterfeiters' side in order to find and exploit the weakest parts of the overall solution. Consequently, all of them should be regarded in combination.

This holistic view even includes specific guidelines for the deployment and introduction of an anti-counterfeiting solution in order to stress the importance of the human factors in the loop and ensure that the solution will actually be used in a real world application as planned on paper. Therefore, apart from recommendations for the integration of the technical infrastructure, topics such as employee motivation, business process integration and even usability issues such as user interface design as

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.4		
Title	Final Application Guidelines for Companies of Different Size	Date	2009-09-29

well as work flow and workplace management are included in the comprehensive list of guidelines published in this deliverable.

1 Introduction

The problem of product counterfeiting is widely recognized and often declared as one of the major threats to businesses. The problem is affecting virtually all industrial areas and has a negative effect on several areas, such as brand value, intellectual property rights, product quality, job market, tax revenue, and consumer and patient safety. Tools for product authentication can help to identify counterfeit products, which helps to eliminate them at an early stage from supply chains and ensures that customers acquire a genuine item. In the past, anti-counterfeiting features on products have often been obscured in order to hide their very existence from potential counterfeiters, which prevented them from being copied as well. The verification of these features has been accessible to experts only and has been applied in exceptional situations only, such as criminal investigations.

One of the goals of the SToP project has been to draw on the potentials of modern identification technologies, which are applied for various purposes, providing value with regard to efficiency, robustness and reliability in many logistics and other processes. These identification technologies, mainly (2D) barcodes and Radio Frequency Identification (RFID), build on open standards and are usually well accessible to all kinds of users. Thus they have the potential to open up anti-counterfeiting functionality to non-experts, thereby creating the possibility to ensure the originality of products at any stage of the supply chain.

The SToP project developed, among others, a technical infrastructure that integrates hardware components, such as reader devices, and software modules that enable product verification. This product verification infrastructure (PVI) was used in industry trials to evaluate it against a specific set of business goals. The industries represented in the project and thus participating in the trials are the luxury goods, pharmaceuticals, and aviation industry. A key objective of this document is to summarize the findings of the SToP project and consolidate the business implications that were primarily drawn from the industry trials.

The rest of the deliverable is structured as follows. Chapter 2 provides background information on the problem domain of counterfeiting. This includes the business drivers that enable trade in fake products, the current approaches in place to counter that, and an introduction to the so-called Auto-ID technologies leveraged in SToP. Based on academic and applied research in the project, Chapter 3 illustrates a holistic approach to anti-counterfeiting. The different steps required in securing a company's supply chain are detailed out and classified into prevention, detection, and response actions. Also, the practical implications derived from the trials are summarized and provided as guidelines for improving different business processes, from production and logistics over retail and analytics to after-incident response. Chapter 4 discusses the SToP implementation of an anti-counterfeiting system which companies can benefit from in the future. Several technical aspects are explained, including feature integration, the overall infrastructure, and the software system architecture. Since anti-counterfeiting cannot be approached from a purely technical perspective, other key aspects are also discussed such as employee awareness, usability, and integration into the established work flows. The document ends with a conclusion in Chapter 5.

2 Background

2.1 The Business of Counterfeiting

Why is the problem of counterfeiting so prevalent? The answer is varying from industry to industry. However, there are some basic incentives for counterfeiters that are present in basically every area. In competitive business environments, brand value is a great asset, and building it requires big amounts of effort and money. Counterfeiters avoid these costs by simply entering the market as a “shadow” company to the original brand owner. They offer a seemingly identical product to the same customer group as the original company. The customers may or may not be aware of the fact that they are being offered counterfeit products; sometimes they even look for them. However, in critical areas such as pharmaceuticals or aviation parts, customers would like to be assured that only high-quality products are on sale.

In most developed countries, serious incidents due to critical counterfeit products are rare. However, the increasing globalization and the opening of markets in developing countries are raising the risks for everybody. Brand owners can often be held responsible if they are not able to provide evidence that counterfeit items are the cause of incurred damage. And even if they are able to provide this evidence, they could suffer serious damage to their image as a provider of high-quality products. Thus, measures that ensure the quality of products and help to identify counterfeits on a global scale are certainly welcomed.

The major drivers for counterfeiters to come up with fake products in virtually all industries is the fact that such products yield high profits and the risks of being held responsible are relatively small. Extreme cases appear when a whole company is being faked, with a wide range of counterfeit products being produced, such as happened with NEC [1]. Modern technology and global trade make it easy to engage in such activities and are the main enablers that facilitate a counterfeit business. For the industries that have been investigated in SToP, Table 1 summarizes the main drivers and enablers of illicit trade. Although differences exist, the main driver is the fact that counterfeiting is a lucrative business if it is exerted professionally. This shows that counterfeiters have to be taken seriously, as they are often well-organized and financially well-equipped.

The role of consumers when it comes to counterfeit products is manifold. Consumers may buy counterfeit goods knowingly or in the belief to purchase genuine products, they may try to ensure to obtain only original articles or invest effort to acquire less expensive fakes, or may even become actively engaged in selling illicit products. In fact, understanding their multifaceted roles is essential for evaluating the implications of counterfeit trade on licit enterprises and for developing effective countermeasures.

A study conducted within SToP revealed that consumers are actually aware of counterfeit products in some industries. Especially fake perfumes, clothing, and watches come to mind when consumers think of counterfeiting. Interestingly, for some products consumers are actually interested in buying counterfeit goods. The study indicates that about a quarter of the population would buy counterfeit clothes, while fake pharmaceuticals and fake food is at the bottom of the list.

Table 1: Drivers and enablers of illicit trade

<p style="text-align: center;">Pharmaceutical industry</p>	<p>The intrinsic quality of a pharmaceutical product is not verifiable by a consumer. Look-alikes are easy to manufacture and distribute, and counterfeiters are hard to track down. Customers are often not aware that they might get counterfeit products.</p>
<p style="text-align: center;">Luxury goods industry</p>	<p>The value of luxury goods is funded on how they are perceived by their owners. Customers are often aware of fakes and acquire them knowingly. Counterfeiting is a profitable business.</p>
<p style="text-align: center;">Aviation industry</p>	<p>In the aviation industry, often parts are being re-used that should have been scrapped. Original parts can be very expensive, so counterfeiters have a high incentive to re-issue old parts. The status of parts is verified based on documents, which can be manipulated.</p>

The primary reported motivation for knowingly purchasing counterfeit goods were the low price for the value of such articles. Being asked "What would be or are reasons for purchasing counterfeit goods?" 65% of the respondents mentioned the high price of the genuine article as a strong or very strong reason, 58% the good quality of counterfeits, and 55% the goods cost-performance ratio of fakes. About 48% claimed

that purchasing counterfeits for amusement or "just for the fun of it" would be a strong or very strong motivation.

Unlike the attitude towards brands, the reasoning for (potential) purchases differed significantly among different consumer groups (i.e. among those who knowingly purchased counterfeit goods and those who did not). The good quality of fakes, the high price of counterfeits, and the attractiveness of brands but the unwillingness to pay the genuine products' price were found to be much stronger motives for those who recently bought imitation products. The findings are in line with other research results, where cost as well as an "acceptable product quality" were the most frequently cited motivations for the purchase of counterfeit fashion items (72% and 60% of the respondents said so, respectively).

Primary reasons against purchasing counterfeit goods were the poor quality of such articles and their limited availability; both motives were more pronounced among counterfeit consumers. Interestingly, the groups assigned similar average scores to the statement "Originals are cheaper on the long run" (32% agreed or strongly agreed). The avoidance of counterfeits due to personal values was significantly more pronounced among those who do not engage in counterfeit purchases (48% agreed or strongly agreed) than among the rest of the group (22% made the same statement).

These results indicate that relying on customers to eliminate counterfeit items from the market is generally not sufficient. Counterfeits should be prevented from reaching the end consumer, thus an approach is required that targets the complete supply chain.

2.2 Anti-Counterfeiting Approaches

The risk of product counterfeiting has forced industries and governments to invest in countermeasures. Many associations and public initiatives fight product counterfeiting on industrial, national, and global levels. One of the most important international forums for anti-counterfeiting is the Anti-Counterfeiting and Trade Agreement (ACTA) currently under negotiation and to be concluded in 2010. Although not undisputed, it will provide an international framework under which the enforcement of intellectual property rights might become easier and more accessible.

Brand owners also want to take measures against product counterfeiting on their own. While some brand owners have a zero tolerance regarding counterfeiting and piracy, others engage in countermeasures on a case by case basis by evaluating the costs and benefits of different courses of actions. In some cases brand owners are even forced to take measures due to external pressure. For instance, a biotechnology company was sued in 2001 on behalf of patients who were sold counterfeit versions of one of its products from reputable pharmacies in California, and the company was pushed to add holograms to help authenticate its products [7].

Many of these decisions are taken on a case-by-case basis. As of today, anti-counterfeiting is a business activity that lacks widely accepted standards. This makes it especially difficult for small and medium-sized enterprises (SME), as they cannot afford to invest in large-scale monitoring infrastructures or dedicated enforcement departments. A proven "best practice" approach is necessary in order to make effective anti-counterfeiting measures accessible to SMEs. We believe that it will still take some time until such an approach emerges, as business operations become more complex and technology advances work in favour of counterfeiters.

For some industries, standard approaches are currently under development. One of the most recent examples is the pharmaceutical industry. The European association of this industry, EFPIA, is undertaking a trial to prove the effectiveness and the usability of a global unique identification system for pharmaceutical products [10]. This activity has been initiated after attempts in several countries to ensure the safety of these products. Since different numbering schemes and authentication features would increase the costs for the production and distribution of pharmaceutical products, a unified and widely accepted approach is now being pursued.

2.3 Auto-ID, RFID and Ambient Intelligence

In general, the term Auto-ID refers to the process of automatic identification of a physical object. Though Auto-ID technologies are mostly used in an industrial or commercial context, they directly benefit also normal consumers and citizens, for example through telephone cards, bank cards, car immobilizers and contactless keys. The most important Auto-ID technologies (based on Finkenzerler [8]) are illustrated in Figure 1.

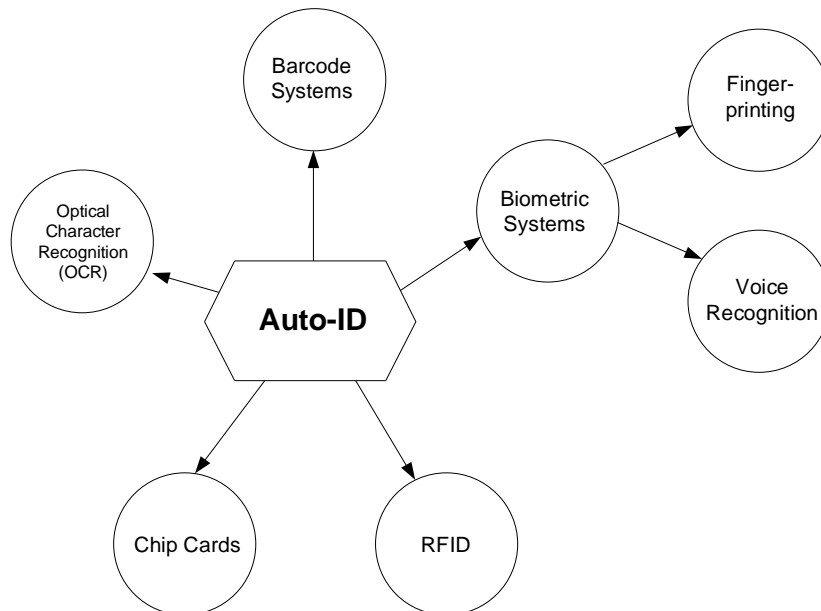


Figure 1. Overview of the most important Auto-ID technologies

The omnipresent barcodes are by far the most common Auto-ID technology today. A typical one-dimensional barcode is a binary code comprising a field of parallel bars and gaps, costs only about one cent to print, and used to identify virtually any kinds of physical commercial products. The most important barcode standards are the 13-digit European Article Number (EAN) and the 12-digit Universal Product Code (UPC). UPC was introduced in the USA as early as 1973 and it was followed by the EAN in 1976. Today, the UPC represents a subset of the EAN code and is therefore compatible with it. There are also two-dimensional barcodes that can incorporate a larger amount of data in a matrix form, such as the Data Matrix. The downsides of barcodes are their relative low storage capacity and the fact that the data cannot be reprogrammed.

Radio frequency identification (RFID) is a contactless Auto-ID technology. Since smart cards can be contactless as well, however, there is a fine line between smart cards and RFID devices, and in this work wireless smart cards are considered as a subset of RFID devices. Though the history of RFID technology dates all the way back to the Second World War, it is only now finding its place as a ubiquitous Auto-ID technology. Being an Auto-ID technology, RFID is mostly used to track physical objects in logistics and retail, but its possible usage scenarios are versatile spanning from animal tracking to ticketing in skiing resorts.

Besides being an Auto-ID technology, RFID is an important enabling technology behind the technology vision of ambient intelligence (AmI). Ambient intelligence refers to a smart electronic environment that is sensitive and responsive to the actors and conditions within the physical environment and it is able to do autonomous decisions that influence the environment. Devices in the ambient intelligence work together to support people carry out their everyday life activities and the concept is closely linked to the societal computing paradigms of Internet of Things (IoT) and ubiquitous computing (UbiComp).

When aligning the development of novel technical anti-counterfeiting measures undertaken in the SToP project, with the technology vision of ambient intelligence, one can foresee a background system that is able to detect counterfeit products automatically in supply chains, without disturbing the users' normal way of work. Making product authentication a continuous background task is a significant paradigm shift in anti-counterfeiting and this document provides application guidelines how it can be achieved.

3 A Comprehensive Approach to Anti-Counterfeiting

3.1 What Kind of System?

Counterfeiting poses a major challenge to any business operation. Everything that benefits the business of genuine brand owners also helps the counterfeiters. The widespread availability of technology simplifies the production processes. The globalization with its offering of cheap transport and available distribution channels makes it especially simple for counterfeiters to push their "products" into markets by free-riding on the good names of highly regarded brands. In addition, the legal remedies are often limited and costly to enforce.

These problems can be approached through different means, and it is the task of a brand owner to select the appropriate mix of technology, jurisdictional forces, and organizational setup that promises the best results.

The advantage of a technical feature is its neutrality and effectiveness. Such a feature delivers the same result no matter who is performing the verification process. It is independent of an ideological framework that might prefer to ignore a negative result. As such, an open technical feature delivers a neutral and objective assessment to all involved stakeholders, including the customer who will eventually consume the product. If well-designed, the verification of such a feature is simple and reliable even in harsh conditions, so a result can be obtained whenever necessary.

There is no shortage of technical product authentication features that are being commercially offered, and we will explain the criteria that are important for the

selection of an appropriate technology in a later chapter. Each technology has implications that lead to persistent changes in different business processes, which have to be taken into account when selecting a technology. The most important decision to be taken is, however, if the integration of a technical authentication feature is necessary at all. In many cases, it will not be sufficient, so jurisdictional and organizational measures need to be put in place as well.

In the following sections of this chapter, we describe the steps necessary to apply a technical countermeasure once the decision for its use has been taken, which must be embedded in the larger context of an organizational and legal framework.

3.2 Securing a Supply Chain

According to the current academic mind-set, security is not a product but a process that combines preventive, detective and reactive countermeasures [2,3]. Interrelated security measures also form the cornerstones of *layered security*, or *in-depth defence*, where security is provided not by one but several measures that come into play if and when the preceding measures fail. This process view, however, is not a dominant perspective within the anti-counterfeiting community that still approaches different countermeasures as distinct silos, often separated by the organizational boundaries of the involved functions within affected enterprises.

The core of the process we describe is constituted by mass serialization concepts and product authentication using RFID. As such, product authentication is not a distinct measure to secure a supply chain from counterfeit products, but rather one part of an integrated process that also comprises several organizational and legal measures. The achieved level of security as well as a counterfeiter's expected payoff from illicit activities are determined by this overall process.

The integrated process of securing a supply chain from counterfeiters is constructed in two steps: first, the steps (threats) that a counterfeiter must perform (materialize) so as to sell a counterfeit product to the secured supply chain are identified, and second, the possible preventive, detective and responsive measures that the licit actors can apply are mapped to this process. Each threat is mitigated by its own *process of security* (prevention-detection-response). It is assumed that all products in the secured supply chain are serialized and the validity of the serial numbers can be easily verified. Moreover, the presented process does not assume that used data carrier for the serial numbers is RFID and therefore the model is valid also for other mass serialization techniques such as 2D barcodes.

The counterfeiter's actions include obtaining counterfeit products, obtaining tags with valid serial numbers, and selling the counterfeit product to the licit supply chain. Obtaining valid serial numbers is in fact not a mandatory step for the counterfeiter, but not doing it enables the counterfeit product to be easily detected based on invalid serial numbers. Therefore also that step is included in the process.

The possible organizational and legal countermeasures are found out from the state-of-the-art anti-counterfeiting best practices and mapped to the integrated process of securing a supply chain. The current best practices are taken from the following studies:

- “No Trade in Fakes Supply Chain Tool Kit” of the U.S. Chamber of Commerce and the Coalition Against Counterfeiting and Piracy [4],

- Benchmarking study of anti-counterfeiting best practices by Staake and Fleisch [5], and
- Intellectual property protection and enforcement manual of the Coalition Against Counterfeiting and Piracy [6].

Figure 2 illustrates the resulting integrated process of securing a supply chain that combines mass serialization-based product authentication as well as organizational and legal measures. Overall, the model shows that a supply chain is secured through three processes (1.1 - 1.3, 2.1 - 2.3, 3.1 - 3.3) that each make it hard for the counterfeiter to achieve his goals. Security is thus not a single process, but a combination of multiple prevent-detect-respond processes. By revealing a broad set of possible points of intervention for licit actors, the model gives a comprehensive view of the available measures that licit actors can apply to secure a supply chain from counterfeits. In addition, the model explains the goals and cause-effect relationships of different countermeasures.

Countermeasures presented in this model are limited to those that directly limit the supply of counterfeit product so the model does not address suppressing of demand or the prerequisites for countermeasures like registration of trademarks and copyrights. Nevertheless, it is the first explanatory models of how a supply chain is secured with a combination of technical, organizational, and legal measures and it can furthermore applied to both licit and illicit supply chains. The different steps in the overall process are detailed below.

3.2.1 Addressing the Supply of Counterfeit Goods

3.2.1.1 Prevent counterfeiters from obtaining counterfeit products (1.1)

The first step in the overall process of securing a supply chain is to make it hard for the counterfeiters to obtain counterfeit products with adequate quality. Though complete prevention is often not realistic, there are ways how brand owners can prevent counterfeiters from exploiting loopholes that can make acquisition of counterfeit products considerably easier. First, precise blueprints of the genuine product should not be disclosed in public. The brand owner can audit manufacturers and subcontractors who provide semi-finished or finalized products to ensure that they are not selling components to illicit manufacturers or running "third shifts" to produce factory overruns.

In addition, manufacturers should verify legitimacy of customers and distributors who might seek to purchase genuine products in bulk only in order to blend counterfeit products among them. This should include guidelines and training the sales force so that suspicious buyers can be identified based on factors such as unusual large volume, cash payment for a very expensive order, order of products that do not fit the customer's line of business, and vague delivery dates and suspicious delivery destinations. Production waste, damaged or unusable inventory, or other inferior goods discarded by the brand owner are also possible sourcing channels for counterfeiters and should therefore be properly handled by establishing policies to confirm proper disposal. Last, the use of seals on containers and smaller consignments can prevent theft that, combined with re-labelling (e.g. marking a later expiry date on perishables, a higher concentration of active ingredient on pharmaceuticals, or a better performance on electronic appliance), can constitute another source of counterfeit products.

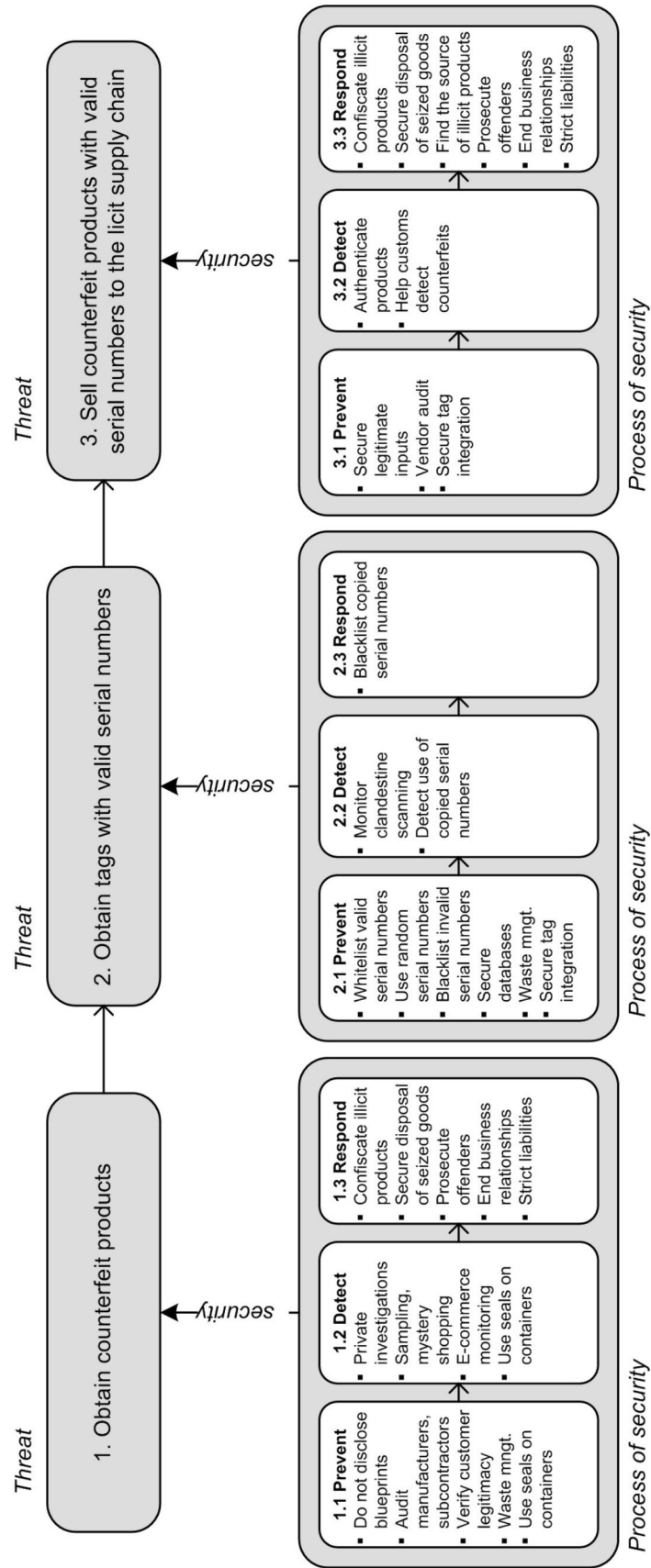


Figure 2: The Integrated process of securing a supply chain against counterfeits

3.2.1.2 Detect counterfeit products outside the licit supply chain (1.2)

Private investigations can be used to detect counterfeit products in a market and to track down their source. Other methods include sampling and mystery shopping where examples are bought from suspicious sources to verify the origins of the sold goods. In addition, brand owners can monitor e-commerce channels including dedicated websites for counterfeit products or "replicas" as well as Internet auction sites. Last, verifying the integrity of seals on containers and consignments helps detect if genuine merchandise is stolen to source counterfeiters.

3.2.1.3 Respond to counterfeiting cases (1.3)

Whenever counterfeit products are detected outside of the licit distribution channels, the illegal goods should be confiscated based on IP right violations. Customs is a critical stakeholder when it comes to supporting seizures. Counterfeit products should be properly disposed of with the help of the manufacturer. In order to demonstrate to those engaged in counterfeiting activities that they are at risk no matter what the level of sales activity, the offenders should be prosecuted even on small counterfeiting cases.

In addition, especially strong brand owners can respond by ending business relationships with offending parties in case such relationships have been established. Last, the brand owner can also employ the concept of "strict liabilities" for instance by including provisions in purchasing contracts to hold sellers responsible for fraudulent goods.

3.2.2 Addressing the Counterfeiting of Serial Numbers

3.2.2.1 Prevent counterfeiters from obtaining valid serial numbers (2.1)

After obtaining counterfeit products it is assumed that a counterfeiter tries to obtain tags (or labels) with valid serial numbers such that counterfeit goods are not being detected in checks. To prevent a counterfeiter from obtaining valid serial numbers, a brand owner should use only a fraction of the available number space for valid serial numbers. In addition, the valid numbers need to be managed in order to prevent their abuse. The first measure is to hold a "white list" of serial numbers that have been assigned to genuine products, such as a manufacturing database. Using random or pseudo-random serial numbers makes it infeasible for a counterfeiter to guess the serial numbers. If possible, a serial number that becomes invalid (e.g. the product is sold or disposed of) can be put on a "black list" of numbers that are no longer valid. These three measures keep the space of valid serial number in minimum size and unpredictable for a counterfeiter.

Furthermore, the databases where the serial numbers are stored should be secured against data theft. In the case where subcontractors are used to label the products, the number of valid serial numbers delivered to the subcontractors should be restricted and controlled to decrease the risk of high-quality factory overruns. In order to prevent removal and reapplication of valid labels from genuine products and their packaging, the waste management of disposed products should be taken care of. Institutional and industrial users such as hospitals represent a critical point for secure waste management. Last, secure tag integration to products can also prevent the removal of labels for illicit purposes.

3.2.2.2 Detect copied serial numbers (2.2)

Detection that a valid serial number has been copied to counterfeit products is important to prevent further counterfeit products with the same serial number from entering the secured supply chain undetected. In principle the use of copied serial numbers can be detected by analyzing track and trace data for inconsistencies, such as repeated sales events. In addition, in case there is an increased risk that a consignment is subject to clandestine scanning for tag cloning purposes in a certain supply chain route, a “logger tag” could be used to register and detect the unwanted communications. This kind of a “logger tag”, however, can be only used with RFID tags.

3.2.2.3 Respond to copying of serial numbers (2.3)

Firstly, valid serial numbers that are known to be copied by counterfeiters should be put on a “black list”. Secondly, the possible supply chain routes or regions where the serial numbers have been copied can be analyzed to help identify the illicit actors.

3.2.3 Addressing the Sales of Counterfeits

3.2.3.1 Prevent from counterfeits being sold to the licit supply chain (3.1)

Measures to prevent counterfeiters from selling fake products to the licit supply chain comprise securing legitimate inputs and vendor audit. This is important especially in the retail level but it also applies to acquisition of raw materials and components. Buyers should be guided how to assess the legitimacy of the supplier, and risk management could be utilized to identify businesses that have an augmented probability of engaging in trade of counterfeit products.

In addition, also technical measures can prevent counterfeit products from being sold to the licit supply chain. For example, assuming that all genuine products must comply to certain tag integration constraints that pose technical challenges (e.g. an RFID tag integrated inside a metal object, or a barcode label sealed with a secure seal), this technical hurdle can be enough to prevent the counterfeiter from obtaining a good that could be sold as a genuine product.

3.2.3.2 Detect counterfeit products sold to the licit supply chain (3.2)

Product authentication can be used to detect counterfeit products as they enter – or after they have entered – the licit supply chain. The assumed product authentication process consist at least of checking whether the product under study has a valid identity, and potentially of also other checks that can detect counterfeit product that bear valid serial numbers. In addition to the authentication of single products, the integrity of consignments can be verified by checking that all the goods are in original packaging, have the same lot numbers etc.

In contrast to the detection of counterfeiters obtaining counterfeit products (step 1.2) and tags/labels with valid serial numbers (step 2.2), detection of counterfeit products inside the licit supply chain can scale up to a 100% detection rate (assuming that all products are checked with a secure method). Furthermore, since the validity of serial numbers can be easily verified as a part of product authentication, the counterfeiter needs to invest in obtaining them – and this can be made hard with steps 2.1 - 2.3 explained above. Therefore product authentication is a particularly important step in the overall process of securing a supply chain from counterfeits.

Product authentication inside the licit supply chain can also be conducted through sampling and “mystery shopping” if the checks need to be conducted without the consent of the seller. Moreover, in addition to conducting the authenticity checks by themselves, the licit supply chain partners should help customs detect counterfeit products by providing them with needed technology as well as information to identify counterfeits.

3.2.3.3 Respond to counterfeiting cases (3.3)

The responsive measures in case a counterfeit product is detected in a licit supply chain are basically the same than those when counterfeit products are detected outside the licit supply chain (step 1.3). They include confiscation of the illicit products, secure disposal of the seized goods, finding the source of illicit products, prosecuting the offenders, ending business relationships as well as applying strong liabilities.

In addition to these measures that affect the counterfeiter's payoff, the response process includes measures that minimize the losses to the licit players, such as informing and warning those who are affected by the counterfeit products. Overall, it is recommended that the internal process for dealing with counterfeiting cases is well established and formalized to enable swift responses as well as gradual improvement of the response process.

3.3 Business Process Set-Up

3.3.1 Production

Object serialization with Auto-ID technologies enables each item to be uniquely identified, a prerequisite for securing supply chains as described in the previous section. The serialization should ideally be integrated as an additional step on the manufacturing line, having several implications on the overall production process. The pharmaceutical trials provided a realistic environment where the implications of object serialization on the production process can be assessed. The scope of the trials included applying the Auto-ID technologies (2D Datamatrix Codes and RFID tags) at the manufacturing lines as well as verifying the features with off-the-shelf reader devices at two pharmacies. Several conclusions that directly affect the production process were reached from both parts of the trial. A particular challenge was to encode data carriers at a high speed – ideally at the maximum line speeds – with tolerable error rates. The testing conducted showed an initial reject rate on the packaging line of 12% which could be reduced to 2.2% after several months of operations. This reject rate leads to discarded packs and requires further improvements to reach limits which may be accepted on an industrial scale. Extensive testing is necessary and the printing technology must be carefully chosen as to not slow down the manufacturing process. Some of the conclusions were only reached by allowing pharmacy employees to verify the serial numbers themselves, using available (non-industrial) readers. For example, off-the-shelf barcode readers were always reading 1D barcodes rather than the 2D variants when both were spatially close on the pharmaceutical bottle. Since the unique item number is encoded on the 2D barcode (in addition to an RFID tag), blocking access to it by the “higher-priority” 1D label is problematic during verification. The list below summarizes key conclusions and implications on the production process:

- Changes to industrial processes are required to enable a serialization process as fast as the current line speeds. The technology requires thorough testing to allow high speed printing.
- Extensive testing and optimization is required to reduce the extent of the encoding errors (e.g. due to dead RFID tags) and bring the resulting defects to a reasonable limit.
- Having more than one Auto-ID feature on the package may prohibit the easy decoding of the serial numbers. Having only one code is much preferable to avoid reading errors. In practice, however, two codes might be required during a transition period.
- 1D and 2D barcodes shall be printed at different spots to avoid confusion by many barcode readers.
- The RFID tag wasn't visible (integrated on the back-side of the label) which resulted in some confusion during the verification stage. An improvement would be to provide some mark that shows where the tag is.
- If more than one technology should still be used for security reasons, they should be read at once with a dedicated device to streamline the verification process.

3.3.2 Transport

Goods in transport as well as transport channels are in danger of being corrupted by counterfeiters, e.g. by replacing genuine items with counterfeits or injecting fake products into licit channels. This applies to linear distribution, where products are manufactured and forwarded to retailers as well as to cyclic processes, such as repeated maintenance and overhaul of spare parts in the aviation industry. It is therefore necessary to protect product paths to prevent and detect manipulations, tampering and most importantly the addition of counterfeits. If the licit transport channels can be kept free of counterfeits, the market for counterfeits is reduced to illicit retailers, which are usually easier to recognize for consumers. It is therefore recommended to add frequent authentication points throughout the supply chain to detect counterfeits early, before they even reach the customer and cause damage, and to make it difficult for counterfeiters to infiltrate distributions channels undetected.

Authentication should take place at every stage of the supply chain, e.g. in warehouses, distribution or service centers. Authentication can be coupled with business process steps such as packing or component dismantling to reduce the overall effort. However, it is important to carefully integrate authentication in these processes to not disturb normal business operations. This requires an integration in existing, process supporting IT systems as well as an easy to comprehend user interface and authentication process. The trials conducted in a distribution center which were integrated with the packing process illustrate how such a seamless integration can be set up.

Potential authentication points in the supply chain are distributed and most often not under control of a single organization. Moreover, each authentication point might have different hardware capabilities and devices. It is therefore necessary to connect disparate authentication points to the central infrastructure, which poses a specific challenge. The device integration modules of the PVI as well as its flexible,

configurable structure and various UI options – including mobile and web-based access – form the technical prerequisites for offering authentication throughout the transport channels.

3.3.3 Retail

Goods are issued to individuals during the retail process. A customer-facing interaction is an important situation for the retailer and for the brand. The goals must be to strengthen the relationship between the retailer and the customer, and to improve or maintain the perception of the brand by the customer. A product authentication process, which could potentially yield a negative result, could surely put these goals at risk. Therefore, it is important to minimize the interference of processes for product authentication and the customer/supplier relationship.

The trials also revealed an important issue about authenticating products in a client-facing situation: Verifying authenticity of products interferes with the customer relationship. In the pharmaceutical industry this is a trust issue between the pharmacist (or the doctor) and the patient. Patients implicitly assume that the products they buy from legitimate sources are authentic without any exceptions and an authenticity check brings a doubt to this assumption. In the luxury goods industry, verifying the authenticity of products at the point of sales “breaks the romance” of the client-facing situation that is built on prestige.

One solution is to authenticate products in the back-office, before they are brought to the shop floor (for retail) or to the point of use. If the integrity of the chain between back-office and point of sales can be guaranteed, however, product authentication in the back-office guarantees the authenticity of goods also at the point of sale or point of use. A critical factor regarding the integrity of inventory is addressing internal threats from employees, for example the possibility of replacing a genuine product by a counterfeit one.

In many cases the retail store is independent from the manufacturer and therefore their might be differing interest and views on who should be responsible for the use of the new system and where it should be used. As shown above, in the pharmacy case, pharmacists might be critical towards a solution making them responsible for authenticating goods at the point of sale. A solution is to involve retail companies as early as possible to identify and clarify under which conditions retailers would be willing to use such a system and what they would be responsible for.

- Authenticate products in the back-office level
- Secure the integrity between back-office and point of sales
- Involve end-user and retail companies to ensure their commitment for the use of the system

3.3.4 Analytics

An anti-counterfeiting infrastructure such as the PVI is a massive data hub, allowing access to anti-counterfeiting relevant feature and tracking data from external systems, as well as creating relevant data itself, e.g. by recording successful and unsuccessful authentication attempts. Analysing the data can serve two primary purposes: 1) item authentication and 2) support of investigation.

For authentication purposes, profiles of the properties of genuine items can be inferred from the data. For authentication, the properties of items under investigation can be compared to the profiles and items with deviating characteristics can be classified as suspicious and be subject to further investigation. Plausibility checks of the history of items represented in the tracking data are an example of this authentication approach. For instance, if it is known that each item is sold exactly once, items with two associated sales events are immediately suspicious.

As a second option, the available feature, authentication and supply chain data can be analysed to monitor and detect trends in counterfeiter activities, detect weak spots in the supply chain, identify collaborators, track down the sources of counterfeits and in general support anti-counterfeiting activities. Suitable methods include visualization, statistics, and data mining. Apart from the authentication, this is one of the key functionalities of an integrated anti-counterfeiting system, which allows gaining a deeper insight into the counterfeiter activities in entire supply chains, across varying product types and countries.

3.3.5 Incident Response

Incident Response is the process of reacting to a problematic event, e.g. a detected counterfeit or a suspicious item. A user or a group of users will be notified about the incident, they will have the possibility to investigate the case, e.g. by analyzing some statistics or background information and to send a message back to the location where the incident happened, e.g. where a counterfeit item was spotted.

As a result of the research conducted within the SToP project it became clear that due to the lack of effective means of identifying many incidents in a timely manner, there is often no well established and formalized incident response process set up that enables appropriate responses.

We thus propose to set up an incident response process that allows selected users to process incoming notifications about suspicious products or detected counterfeits in an automatic fashion, e.g. through a PVI After Incident Management module sending messages containing comprehensive instructions to the locations where counterfeits have been detected and how to process them to a previously determined set of relevant users.

The process should ideally be well integrated with the standard notification procedures defined in an ERP system or at the least with the respective communication infrastructure, such as e.g. an Exchange server, so that processes outside the domain of a PVI system can be triggered accordingly. Due to the fact that our investigations have not identified stable patterns of counterfeiting incidents across industries, the incident response process should mostly be concerned with notifications without much business process automation beyond them, since a human evaluation and processing seems appropriate due to the sheer number of variations among different incidents. Therefore, the process should allow for a timely, easy and semi-automated processing of suspicious incidents or detections of counterfeits. As it is expected that many more counterfeits and suspicious activities than today will be detected once a verification infrastructure is in place, a second step should be to investigate more elaborated process support with the aim of standardizing the today often unstructured investigation process. In any case it must be ensured that notifications about suspicious events or the detection of counterfeits are forwarded to the responsible parties as well as to provide a back-channel that allows those parties to

communicate with the people on-site, e.g., to instruct them on how to handle the incident.

The After Incident Manager as it was specified for the PVI within the SToP project is already well suited as a basis for implementing an incident response business process as recommended above, if integrated with the respective enterprise systems.

To summarize, we recommend taking the following steps for incident response:

- Identify responsible parties for counterfeit incident response. These positions must be empowered to take appropriate action, which might include the involvement of law enforcement agencies.
- Identify parties that should be notified about counterfeit incidents, but which are not responsible for actions. Reporting incidents is a sensitive issue, however accurate statistics may help to coordinate efforts against counterfeiting across organizations.
- Establish workflows that ensure the delivery of notifications about incidents and that allow timely reaction.
- Implement workflows with the support of information and communication infrastructures such that relevant data is available for information exchange and reporting.

3.3.6 Protection of Intellectual Property

According to the World Intellectual Property Organization (WIPO), intellectual property (IP) refers to “creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.”¹ Intellectual property – ideas and knowledge – is an increasingly important part of trade; most of the value of new medicines, high technology products, films, music recordings, books, software, branded clothes or new varieties of plants lies in the amount of invention, innovation, research, design and testing, or information and creativity involved. Not to mention brands.

Intellectual property rights (IPR) grant inventors and authors the right to prevent others from exploiting their intellectual property, usually giving the creator an exclusive right over the use of his or her creation for a certain period of time. Intellectual property rights come in many flavours the most important of which being patents, trademarks, copyrights, geographical indications, and industrial designs (cf. Table 2)². These are described below based on WIPO [9].

- Patents protect inventions as new solutions to technical problems. Merely discovering something that already exists in nature is not an invention but human intervention must be added, as well as industrial applicability and non-obviousness. Patent gives an exclusive right to the invention. In return for the exclusive right, the inventor must adequately disclose the patented invention to the public.

¹ <http://www.wipo.int/about-ip/en/>

² In addition, intellectual property rights cover layout-designs of integrated circuits and plant variety rights of breeder of a new variety of plant

- Trademarks are signs which distinguish the goods or services of one enterprise from those of another and they are targeted for consumers. They can use words, letters, numerals, pictures, shapes and colours, or any combination thereof. Furthermore, some countries allow for the registration dimensional signs (e.g. the Coca-Cola bottle), audible signs (e.g. the lion roar that precedes MDM films) or even olfactory signs (e.g. perfume smells). Trademarks are used to protect brands that are the essence of a competitive economy. They differentiate offerings through innovation which makes them relevant to the consumer.
- Copyrights protect results from intellectual activity in the industrial, scientific, literary or artistic fields, such as books, music, paintings, sculptures, and films. They grant authors have the exclusive right to authorize public performance, broadcasting and communication of their works to the public. The duration of a copyright provided for by national law spans in general at least 50 years after the author's death.
- Geographical indications are signs used on goods that have a specific geographical origin and possess qualities or a reputation that are due to that place of origin. They may be used for a wide variety of agricultural products, such as "Tuscany" for olive oil produced in a specific area of Italy, or "Roquefort" for cheese. Geographical indications may also highlight particular qualities of a product, which are due to human factors found in the place of origin of the products, such as specific manufacturing skills and traditions, such as "Swiss made" for watches.
- Industrial designs are ornamental or aesthetic aspect of useful articles considering shape, pattern or colour the article. They recognize and protect the visual appeal of products. Industrial designs can generally be protected if they are new or original. The usual maximum duration of an industrial design is from 10 to 25 years, depending on the country.

Today the protection of intellectual property rights in the international trade is governed by the Agreement on Trade-related Aspects of Intellectual Property Rights, TRIPS³. TRIPS agreement was negotiated in 1986-94 and they introduced for the first time intellectual property rules into the multilateral trading system. It establishes minimum levels of protection that each government has to give to the intellectual property of fellow WTO members.

Table 2. Summary of intellectual property rights [9]

Right	Description	Example subjects
Patent	<ul style="list-style-type: none"> • Protects inventions, both products and processes • Exclusive rights to the invention generally for 20 years • Regional validity, differences in legislation 	Viagra, Paper clip, Light bulb
Trademark	<ul style="list-style-type: none"> • Protects words, letters, pictures, shapes, colours etc. 	Coca-Cola label,

³ WTO (1994). Agreement on trade-related aspects of intellectual property rights (TRIPS). World Trade Organization. <http://www.wto.org/english/tratop E/trips e/trips e.htm>.

	<ul style="list-style-type: none"> • Distinguishes goods or services to consumers • No fixed expiry time (re-registration) 	Coca-Cola bottle
Copyright	<ul style="list-style-type: none"> • Protects books, music, paintings, sculptures, films etc. • Exclusive rights to encourage and reward creative work • Valid at least 50 years after the death of the author 	Beatles songs, Harry Potter books, MS Office
Geographical indication	<ul style="list-style-type: none"> • Protects signs indicating specific geographical origin • Highlights qualities, reputation, manufacturing skills, and traditions specific to the place of origin 	Swiss made, Roquefort, Havana
Industrial design	<ul style="list-style-type: none"> • Protects aesthetic aspects, shape, pattern or colour • Right to prevent the manufacture, sale or importation of copies of the protected design 	Mobile phone, User interface

4 Implementation

4.1 Anti-Counterfeiting Measures

Brand owners have different anti-counterfeiting approaches in their arsenal. These approaches are summarized in Figure 3 and they include consumer information and education, legal actions, private investigations and cooperation with enforcement agencies, and technical counter measures. The goal of consumer education is to decrease the demand for counterfeit products and increase the awareness of negative effects of counterfeiting. This measure is blunt and somewhat inefficient and mostly adopted by associations and governments instead of single brand owners.

The goal of legal actions is to prosecute and punish counterfeiters and confiscate their illegally-financed assets. The downside of legal actions is that they might not scale to solve the problem because most counterfeit players cannot be detected and prosecuted. Furthermore, even if detected, counterfeit players are not always prosecuted due to lacking law enforcement in their countries of origin, and the fines due to illicit trade can be small compared to the illegal profits. Therefore legal actions are currently seen mostly as a basic prerequisite for brand protection [5].

The goal of private investigations and collaboration with enforcement agencies, such as customs, is to support seizures of counterfeit products and detection and prosecution of counterfeiters. And last, the goal of technical measures is to help brand owners prove the origins of goods, for example in a legal case, and to protect the licit supply chain.

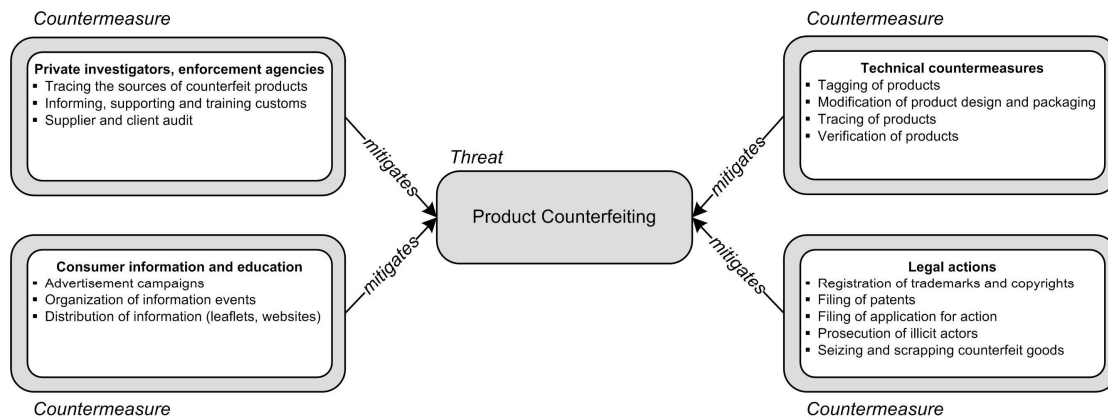


Figure 3. Summary of existing approaches to fight product counterfeiting

We are concentrating on the implementation of technical countermeasures in this chapter, as this has been the focus of the SToP project. For the other topics, we refer to additional sources, such [4,5,6,7].

4.2 Feature Selection and Integration

There is a wide variety of commercial products being offered for product authentication, product and item identification, and product protection. Often, they rely on similar technologies and combine these technologies in specific ways. Thereby, they can offer different security “guarantees”.

A number of criteria are important for feature selection. Table 3 shows these criteria for several technologies. The first obvious criterion is visibility, reflecting the need of a technology to be attached and being visible or invisible to the human eye. For visible features it is interesting to see whether these can be integrated into products and what consistencies are supported.

Looking at the process of attaching a feature or capturing product characteristics, some technologies need more space on the product or packing than others. Some technologies under direct authentication do not need any space at all, but Laser Surface Analysis, for example, needs space of about two to three centimetres, even if it is a direct authentication technology. Furthermore not all product consistencies are supported, for example usage of RFID tags with products containing metals can be cumbersome as interference arises. Product consistence is an important criterion, eliminating non-appropriate technologies. Another differentiating criterion is the supported speed and automation during authentication. Some technologies allow for automated and speedy authentication, whereas others require manual processing. This is heavily related to the technologies’ maturity, as only some are already in industrial use. As speed comes with automation, only the criteria authentication speed is kept.

Some technologies also need a further means for authentication. Some of the technologies are directly usable by people, whereas others need standard or special devices. Furthermore, some technologies do not come with sufficient data capacity to work without a network.

All technologies come at some cost. Cost is partly dependent on the logic used and on the technology itself, e.g. cost for RFID tags. The same is true for the security aspect. A logic offers a certain degree of security, which is complemented by the underlying technology. Here it is of interest in how far the security level is adaptable and how

these changes can be performed without confounding the user. Security has not been noted as a criterion as it is mainly dependent on the vendor and a general assessment is impossible to give. Also it is not within the chosen level of analysis in this thesis.

Some of the technologies used for authentication can also be used for identification. For identification, no security is required, but high efficiency and ease-of-use. Not many technologies provide these properties; only barcodes and RFID are commonly used for (unique item) identification.

This combination of functionality has a great appeal, as it would keep costs low, as two different services could be provided using the same instalment.

The actual integration of security features might be tricky, especially if the feature should be applied to the item itself but must not interfere with the item's purpose. This is important, for example, in the case of watches. The visible design must not suffer because of the integration of an identification and authentication feature. So the existing product design must be investigated, an approach needs to be found, such as in the following example.

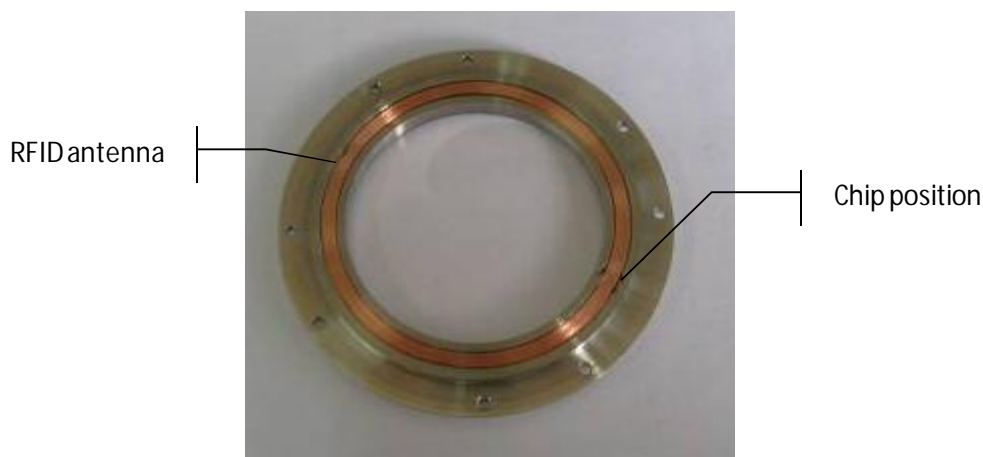


Figure 4: RFID tag integration in a watch frame

The analysis of the watch showed that it would be possible to integrate an RFID tag into the metallic part of the case but only after creating a special groove to accommodate it. In order to still comply with the mechanical constraints of the watch assembly, the watch maker had to define the exact size of the groove to be created in the metallic casing. Figure 4 shows the end result with the RFID tag (antenna and chip) nicely embedded in the watch frame.

Table 3: Criteria for technology selection

Authentication Technology	Criteria							
	Authentication Device	Data Capacity	Supported Product Consistence	Visibility	Required Space	Authentication Speed	Feature Integratability	Cost
<i>Forensic Analysis</i>	Special Device	None	All	No	None	Low	-	High
<i>Photo Comparison</i>	Photo Camera	None	All	No	None	Medium	-	Low
<i>Laser Surface Analysis</i>	Special Device	None	Paper, Metal, Textile, Plastics	No	2-3 cm	Medium	-	Medium
<i>Security Printing</i>	No Device	None	All	Yes	< 2cm	Medium	No	Low
<i>Hologram</i>	No Device	None	All	Yes	< 2 cm	Low	No	Vendor specific
<i>Hologram with stored Data</i>	Special Device	Low	All	Yes	< 2cm	Low	No	Vendor specific
<i>Copy Detection Pattern</i>	Special Device	None	All	Yes	2-3 cm	Medium	No	Low
<i>Copy Detection Pattern with Data</i>	Special Device	Low	All	Yes	2-3 cm	Medium	No	Low
<i>Micro Wire</i>	No Device	None	Paper, Textile, Plastics	Yes	2-3 cm	Low	Yes	Low
<i>Micro Wire with stored Data</i>	Special Device	Medium	Paper, Textile, Plastics	Yes	> 3 cm	Medium	Yes	Low
<i>Barcode (1D)</i>	1D Barcode Reader	Low	All	Yes	2 - 3 cm	Medium	No	Low
<i>Barcode (2D)</i>	2D Barcode Reader or Photo Camera	Medium	All	Yes	2 - 3 cm	Medium	No	Low
<i>Micro Print</i>	Special Device	Low	Paper	No	< 2 cm	Medium	-	Low
<i>Polymer Material with stored Data</i>	Special Device	High	All	No	> 3 cm	Medium	Yes	Low
<i>Class 0 – I RFID Tags</i>	RFID Reader	Medium	All, Interference with Metal and Liquids	Yes	2 - 3 cm	High	Yes	Low
<i>Class II – IV tags Tags</i>	RFID Reader	High	All, Interference with Metal and Liquids	Yes	2 – 3 cm	High	Yes	Medium

4.3 Verification Infrastructure

4.3.1 Technical Infrastructure

The technical infrastructure that is the basis for product authentication consists of the system for product authentication, authentication terminals (e.g., stationary PCs, tablet PCs, mobile phones, etc.), which are the execution environment for authentication clients (e.g., web browsers or standalone applications), and authentication devices (e.g., barcode scanners, RFID readers, LSA scanners, etc.). Figure 5 shows these basic components as well as two device integration scenarios. The core of the technical infrastructure is the system for product authentication, which is not necessarily a central system but could also consist of distributed components. Authentication terminals are connected to the system for product authentication over a network or the internet and are both able to run authentication clients and integrate authentication devices. An example for an authentication terminal is a stationary PC that runs a web browser, which represents an authentication client. Using this browser a user can access the system for product authentication through a web application, which is offered by an HTTP server. Another example for an authentication terminal is a mobile phone, which runs a Java application that communicates with the system for product authentication through TCP/IP.

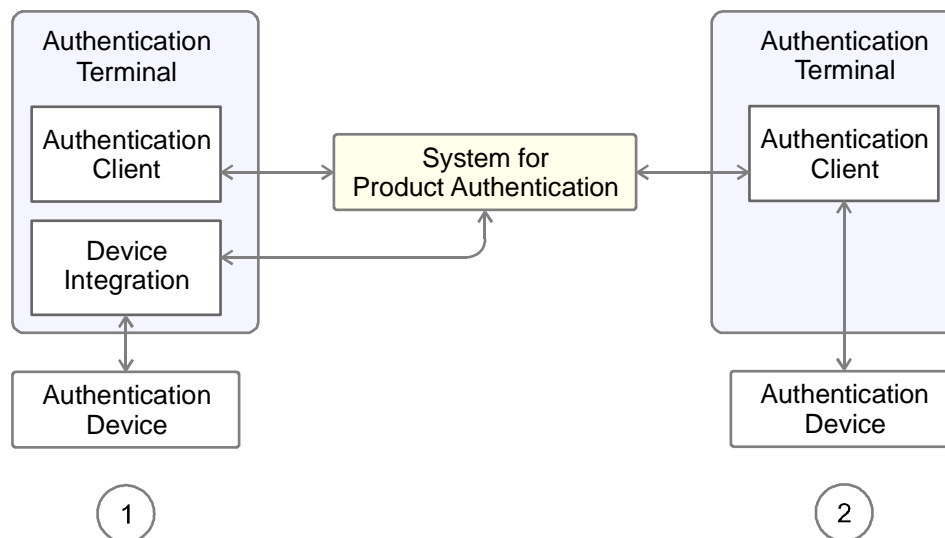


Figure 5: Basic Components of the Technical Infrastructure

Finally, authentication (or reader) devices are connected to authentication terminals. Figure 6 shows several devices that are used to authenticate products, i.e. features that are attached to these products. If the authentication client is a web browser, it cannot directly communicate with authentication devices, as this would break the sandbox principle. Thus, a device integration component, which also runs on the authentication terminal, is responsible for exchanging data between authentication devices that are locally attached and the system for product authentication (cf. scenario 1 in Figure 5). The communication between the device integration component and authentication devices is device-specific, whereas the communication between the device integration component and the system for product authentication is device-independent. To integrate an authentication device, a driver is needed that adheres to the specification required by the device integration component. If the authentication client is a

standalone application, authentication devices can also be directly integrated into the client (cf. scenario 2 in Figure 5). An example for this scenario is a mobile phone with an integrated RFID reader that runs an authentication client in the form of a Java application.



Figure 6: Reader devices

4.3.2 Employee motivation and awareness

Even though the problem of counterfeiting is well acknowledged within industries and single companies, trials with real end-users discovered that there is no “pain” felt about counterfeits in the grass root level and that many employees don’t have a thorough understanding of the problem. Counterfeiting is perceived as a problem that only affects the management of the company or is only present on the Internet or flea markets, but it is not seen as a problem that affects the licit supply chains. This lack of “pain” and understanding can make employee motivation extremely challenging since they do not perceive or understand the benefits of improved supply chain security.

Informing and educating about the problem of counterfeits is the first measure to be taken. It increases their motivation to guarantee a safe and secure supply chain and is expected by the employees.

In optimal usage scenarios, authentication is integrated to identification processes in such a way that it does not represent additional overhead or effort for the users. The new system should also be used at the same place or as replacement of already existing systems (e.g. stock management systems). A seamless integration into or replacement of already existing system would not disturb their current handling processes and therefore positively impact on their motivation. In addition the new system should be at least faster than the replaced system. This is a very good way to address the lack of motivation to verify products. If it is not possible, employees can be motivated to verify products also by providing them additional information and thus additional benefits from scanning products. These benefits are case specific but the additional information is typically item-specific data such as expiry date, warranty, service history etc.

- Inform about counterfeits
- Integrate authentication to identification
- Provide additional benefits from scanning the items (expiry, warranty, service history etc.)

4.3.3 A System for Product Verification

In the SToP project, the data and functionalities for product authentication have been encapsulated in a system called the *Product Verification Infrastructure* (PVI). The PVI architecture (Figure 7) provides an overview of what modules must be present in such a system and how they interact. Pre-authentication modules are responsible for collecting data about events that are relevant to authentication, and they support the creation of authentication features, such as unique serial numbers or printed tags with encoded data. Sometimes, such components come from external vendors, who will support the creation of tags through proprietary algorithms.

Authentication modules analyze the collected data and perform the verification of security features. Thereby the authenticity status of an item is being determined, a process that sometimes does not lead to a definitive result but in a probability. Depending on the context of the verification process, a certain action will be taken, which is the responsibility of the operational modules. These interact with the users, possibly alerting them about detected counterfeits and providing instructions on how to handle them.

In an enterprise context, reporting is an important task in order to keep management aware of the business operations. Information about detected counterfeits may trigger further actions within an organization, such as immediate response to an incident (e.g. sending a field investigator), or the re-consideration of organizational measures according to statistics about counterfeit products.

The PVI design has been validated by a prototype implementation, which supports most of the functionalities described. The prototype has been adapted to different application scenarios and tested in field trials. As such, it serves as a blueprint for a full, deployment-ready implementation.

A PVI-like system could be operated as part of the IT system of a brand owner. Product data needs to be synchronized with the product master data, and event data can be drawn from the logistics event repository. Depending on the number and type of clients (e.g. mobile computers or partner systems) the management of such a

system could significantly increase the complexity in the IT department. The dependency on external verification services, which is a prerequisite imposed by some feature providers, would increase this complexity further.

An alternative approach is the operation of the system as a service. The complexities imposed by system dependencies and client management would thereby be shifted to a specialized provider. This would potentially lead to efficiency gains, which would result in a lower total operational cost and therefore reduce the costs for brand owners. However, business-critical data would have to be handed to a service provider then, which may not be acceptable in some cases. Also, interfaces for exchanging product master data and events must be created and maintained.

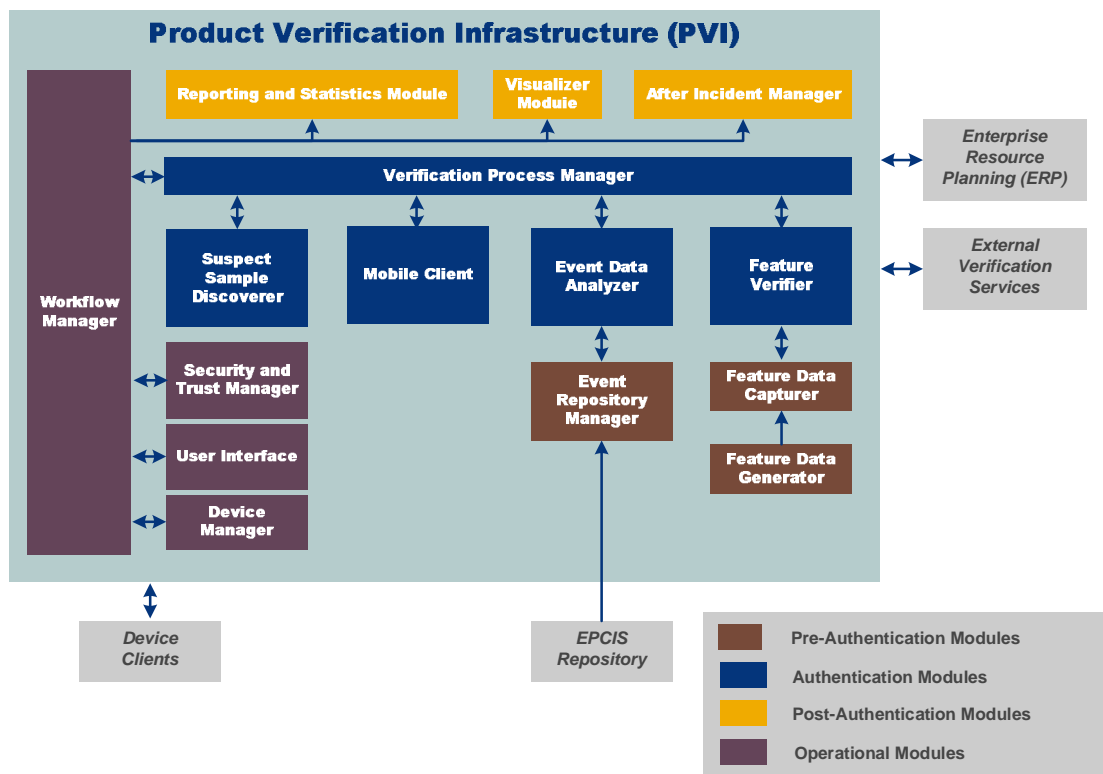


Figure 7: General architecture of a system for product verification

To our knowledge, no complete offering of such a system is on the market as of today. Basically, all components are available but need to be integrated. Probably, some vendors will emerge in the future offering ready-made integrated solutions and also operating the underlying infrastructure.

4.3.4 Business System Integration

A system for product verification would not be operated as a stand-alone system but it would require permanent interaction with other business systems. The integration between the PVI and external systems can occur in both directions: either the PVI acts as a server when external systems require e.g. PVI checks and also as a client when the PVI requests Track & Trace data that is already captured by other systems. As an example, we discuss the integration with a warehouse management system (WMS). The WMS under consideration has the capability to store track & trace data. When a company already has this data captured and stored in the WMS, the PVI can connect

to the latter and request the needed data. The WMS processes this request and sends data back to the PVI.

For example, when a company receives goods and the PVI responds that the goods are counterfeit, there are different options, depending on the business rules in place. In most cases further actions need to be taken, e.g. marking the products in the WMS with the quality mark “counterfeit”. These product cannot be handled further (e.g. ship them or use them in a process) until the “counterfeit” mark is cleared again. When we are sure that an item is counterfeit further legal actions towards the supplier can be triggered depending on business rules, which can be specified in the WMS or the PVI. Note that the application semantics in this case is part of the WMS. If application-specific actions need to be taken, the WMS should therefore specify them, while general actions can be specified within the PVI.

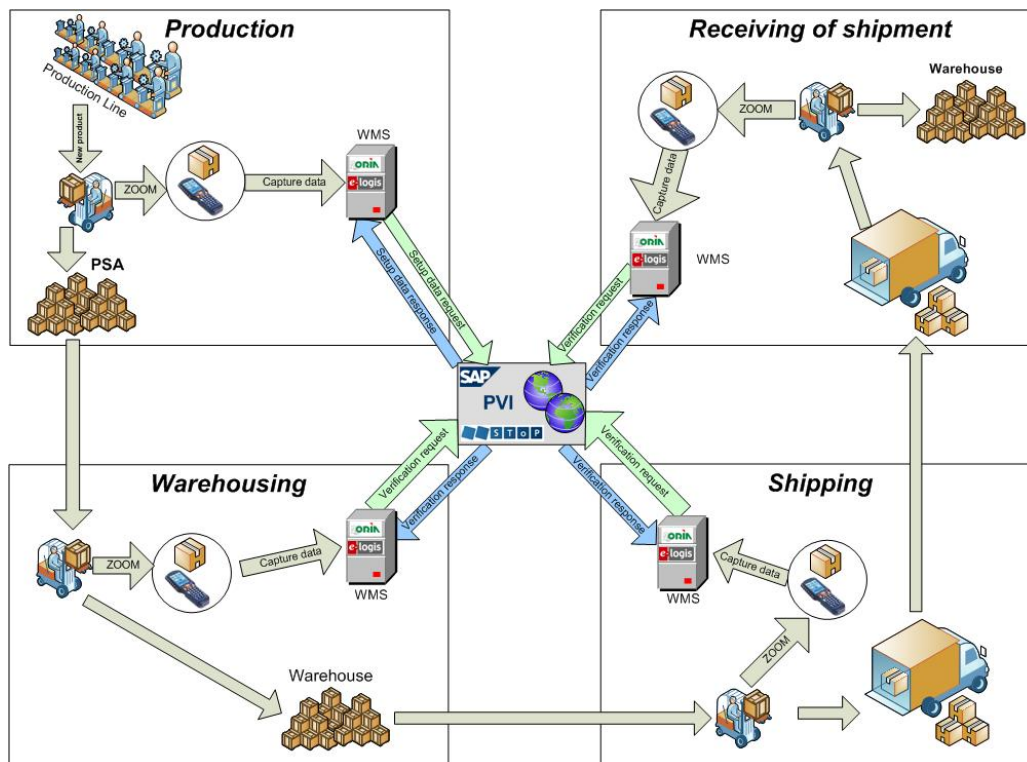


Figure 8: Business processes accessing product verification

This scenario shows that authentication events can be handled by a business system in a straightforward way. A flexible business software system should have no problems integrating the results of the authentication service. Details, however, are organization-specific, such as the definition of rules based on authentication results.

One important aspect is the exchange of authentication information between companies. For example, a shipping company or a retailer could notify the manufacturer if non-authenticated items are being detected. This is a sensitive process since such a situation could reveal or at least imply bad business practices at the shipper or retailer. Thus most companies would be reluctant to share such information freely. It is a different matter, of course, if a neutral party, such as customs, or a contractor performs authentication. In these cases, notifying the brand owner would be a prerequisite for collaboration.

4.4 Usability

4.4.1 User Interface

The real-world trials discovered a problem with the user interface. Though the authenticity results were always presented on the screen in an unambiguous way, the users did not find it always easy to accomplish their designated tasks while authenticating products. Overall, the goal of the SToP-approach is to have an integrated IT system for authenticity checks and not a separate device that simply displays green-light / red-light. Therefore the user interface must be linked to the ongoing tasks and activities and it must, at every point of time, answer the user *what must I do next*. Observations and interviews in the trials suggested that this is the only piece of information that the users really need and expect the system to tell them. Almost everything else can be hidden and displayed as additional details when demanded. In general, the user interface must be linked to the work flow.

Different users react in different ways to acoustic and visual feedback; while some users always want to verify the screen after scanning a product to see the “real result”, other users concentrate on the beeps that the system makes and think that the screen shows only additional information. Because of these differences, both acoustic feedback and visual feedback are needed. Furthermore, the primary feedback channel depends heavily also on the task and the ergonomic setting of the work environment.

The user interface also needs to provide a link between the read events captured by the system and the physical products. Though RFID systems are able to handle physical items as visually identical units, the users want to see a link between a read event on the screen and a physical product on the table. This is especially needed for error handling and removal of uncertainty regarding which product was scanned, and it makes radio frequency identification “visual”. And in case an error occurs (e.g. a wrong product is scanned), the system should support for manual corrections and manual data entry. This does not only enable smoother handling of exceptional cases, it also increases the users’ feeling of being in control.

The user interface is also closely linked to a security policy. For instance, if a consignment contains two products that have the same EPC number (e.g. one of the products is a counterfeit with a cloned tag) and these products are scanned, the system will see the same number scanned twice. In this case the system is not able to tell if one single same product was scanned twice, or if there are two products with the same EPC number. To handle this case so that the cloned tag is detected, the RFID middleware must be configured so that it does not filter out the second read event, and the system should allow scanning the same item twice but display a warning message where the user needs to confirm that the scanned item has already been scanned before. If scanning the same item twice is not allowed, the system is blind to duplicated EPC numbers within consignments.

- User interface must always answer *what must I do next*
- Link user interface to work flow
- Both acoustic and visual feedback are needed
- Link the read event with a physical product to foster the feeling of being in control
- Educate about reading range of wireless systems

- Allow manual corrections, manual data entry
- Allow users to scan same item twice

4.4.2 Work Flow and Workplace Management

The trials revealed that work flow management requires very careful attention when designing how the product authenticity checks are to be used. Integration of identification and authentication modifies the existing work flows more than a simple check that displays a yes/no result. These changes need to be anticipated and trialed in order to have very clear and precise work flow descriptions that the users understand and that cover all possible cases and system states.

In order to manage the read ranges of reader devices, users need to be explained where and when the RFID-tagged products can be placed. If possible, the areas where tagged products can be placed while completing a task should be clearly marked e.g. on a table or on the floor. This can greatly reduce the chances of getting “ghost reads”. If RFID is used, the work flow description needs to be precise enough to even tell how many products the users can hold in their hands, and in which hands, to make sure that the right product is scanned. In addition if several products are scanned at once and one is a counterfeit, users need to learn how to properly identify a counterfeit. The rules should not be too limiting for the users, however, since they typically want to perform the tasks fast and smoothly, and discover ways to optimize the way they handle the products.

If an incident occurs, for example a counterfeit product is detected, the work flow should be halted and explicit user feedback should be asked for. Such incidents are considered rare and important, and therefore they do not need to be handled in a particularly fast or easy manner. In these cases the user can be expected to give for example manual input that otherwise is avoided, but the system must nevertheless allow the users to finish the tasks. Furthermore, the process for incident handling must be defined and known by the users. The supervisors are typically very closely involved in handling the incidents. Still they need to know what to do next and who needs to be informed about the incident. Last, in case there is no electricity or Internet connection, the work flow should also include a fall back plan that enables finishing of business-critical tasks even without the support of the IT system.

- Have very clear and precise work flow descriptions
- Explain and mark where the RFID-tagged products can be placed
- Provide clear information about the products in the reading range
- If incidents occurs (e.g. counterfeit), halt the work flow and require explicit user feedback
- Define process for incident handling
- Fall back plan in case no electricity or Internet connection

5 Conclusion

The presented technical solution represents a significant paradigm shift in anti-counterfeiting since it renders product authentication from a special task requiring

specialized device to a background task that is done automatically every time when products are automatically identified. The value of such a technical solution for affected companies is a complete coverage of authenticity checks with a minimal effort.

Moreover, these application guidelines describe in details how technical countermeasures are interlinked with organizational and legal measures to secure a supply chain against counterfeit products through multiple prevent-detect-response processes.

Naturally, the implementation of the complete set of application guidelines outlined in this document is neither trivial nor cheap, as each organisation is bound within the constraints of the status quo with varying degrees of control over its supply chains and business partners and with even less control over the legal aspects of anti-counterfeiting related issues.

The technical foundation of a comprehensive solution as the PVI contributed by the SToP project including the overall technical strategy and the appropriate choice of security features is as such the least problematic to implement. The implementation guidelines presented in this deliverable provide a systematic and concrete approach for all relevant technical issues. Together with a planning and evaluation tool as the one provided in WP2 diverse organizations of different industries can easily develop their technical strategy that, taken together with a feature-agnostic authentication platform such as the Product Verification Infrastructure (PVI) whose architecture is a major contribution of the SToP project, provides a solid foundation for adapting to the inevitable future technical changes in security features. In this respect, the feature selection guidelines provided in this document remain adaptable even if technical requirements change over time. However, as outlined above, the technical countermeasures have to be interlinked with organizational and legal measures, in order to become effective.

The changes within the organization might be more difficult to implement than the technical foundation and the results from the SToP trials already indicate the importance of organizational change, despite the limited scope of the trials. Extrapolated to the reality of larger organizations we cannot overestimate the crucial effects of cross-organizational change management. Employee motivation and workplace management must not only be taken seriously, but the technical system must be designed in a minimally invasive way in order to prevent renitent tendencies among the involved personnel. The focus on emerging ambient intelligence technologies that support implicit interaction and automatic background behaviour has thus remained promising throughout the execution of the SToP project.

While agile and fast moving organizations will succeed in implementing the technical and intra-organizational guidelines presented in this document, the biggest challenge however will relate to securing the supply chain including the sales of counterfeit products. Depending on the openness of licit supply chains and the degree of control that can be exerted over business partners, securing the supply chains and the related adaptation of business processes and transactions between partners require the momentum of industry leaders and possibly also industry specific initiatives that bring together the major players in any given industry. At this scale, the guidelines presented here are less relevant than on the individual organization and supply chain level. When it comes to industry spanning solutions and ultimately to European

Project Title (Acronym)	SToP Tampering of Products (SToP)	Project Number	IST-034144
Deliverable	Deliverable 5.4		
Title	Final Application Guidelines for Companies of Different Size	Date	2009-09-29

consumer protection, a joint legislation and EU-wide initiatives beyond individual organizations are required for the benefit and protection of the European citizen.

6 References

- [1] New York Times (online edition): Next Step for Counterfeiters: Faking the Whole Company. 01 May 2006, <http://www.nytimes.com/2006/05/01/technology/01pirate.html>
- [2] Schneier, B. Computer Security: Will We Ever Learn? Crypto-Gram Newsletter, May 15, 2000.
- [3] Schneier, B. Beyond Fear. Thinking Sensibly about Security in an Uncertain World. Copernicus Books, Springer-Verlag, 2003
- [4] No Trade in Fakes Supply Chain Tool Kit. US Chamber of Commerce, The Coalition Against Counterfeiting and Piracy (CACP), Accenture, 2006.
- [5] Staake, T. and Fleisch, E. Countering Counterfeit Trade – Illicit Market Insights, Best-Practice Strategies, and Management Toolbox. Springer-Verlag, 2008
- [6] Intellectual Property Protection and Enforcement Manual: A Practical and Legal Guide for Protecting Your Intellectual Property Rights. The Coalition Against Counterfeiting and Piracy (CACP), 2009
- [7] Hopkins, D., Kontnik, L., and Turnage, M. Counterfeiting Exposed: Protecting Your Brand and Customers. Wiley, 2003
- [8] Finkenzeller, K. RFID-Handbuch - Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. Carl Hanser Verlag, 2006
- [9] WIPO (2004). Understanding Industrial Property. World Intellectual Property Organization. http://www.wipo.int/freepublications/en/intproperty/895/wipo_pub_895.pdf (09.07.09).
- [10] EFPIA announces launch of anti-counterfeit coding pilot project in Sweden. EFPIA press release, 15 May 2009. www.efpia.org