European Commission

JRC TECHNICAL REPORTS

Survey of techniques for the fight against counterfeit goods and Intellectual Property Rights (IPR) infringement

Gianmarco Baldini
Igor Nai Fovino
Riccardo Satta
Aris Tsois
Enrico Checchi

2015

EUR 27688 EN

Joint Research Centre

JRC Science Hub
https://ec.europa.eu/jrc

JRC98181

EUR 27688 EN

ISBN 978-92-79-54544-3 (pdf)

ISBN 978-92-79-54543-6 (print)

ISSN 1831-9424 (online)

ISSN 1018-5593 (print)

doi:10.2788/97231

How to cite: G. Baldini, I. Nai Fovino, R. Satta, A. Tsois, E. Checchi; Survey of techniques for the fight against counterfeit goods and Intellectual Property Rights (IPR) infringement; EUR 27688 EN; doi:10.2788/97231

Table of contents

Acknowledgements:

The authors acknowledge and they are thankful for the comments and recommendations provided by DG GROW/J/2 (Jean Bergevin and Stephanie Martin), the Office for Harmonization in the Internal Market (OHIM) (Andrea De Carlo, Massimo Antonelli, Valerio Papajorgji), UNICRI (Marco Musumeci), Reconnaissance International (Ian Lancaster), Brandstrike (Damian Broker), Indicam (Claudio Bergonzi, Sara Gabri), Philip Morris (Tamas Sipos, Kacper Chmielewski) and other representatives from the OHIM Observatory.

Abstract

The objective of this report is provide a survey on the techniques (i.e., technologies and procedures) that can be used in the fight against the distribution of counterfeit goods in various domains. Different techniques can be used to identify and control the distribution of counterfeit goods at different levels. The list of surveyed techniques and approaches in this report includes: a) technologies for goods authentication, which can be used to distinguish between genuine and counterfeit goods, b) track and trace technologies, which can be used to control the supply and distribution chains to make it easier to detect counterfeit goods in the supply chain entering through a legitimate distribution channel, c) technologies and procedures for container tracking and sealing c) technologies for the analysis of ecommerce web sites, which can be used to identify sellers of counterfeit products and d) set-up of organizational structures and processes.

Each technique may not be the only valid solution for the problem of production and distribution of counterfeit products. The problem of counterfeiting is related to many different domains and goods (e.g., agricultural products, electronic circuits, medicines) and each technique can be applied with different degrees of success to different domains. In addition, each technique has a different level of market maturity: some techniques are still in the research stages while others have been already deployed in the market for years. The survey evaluates and compares the techniques against the different domains using different metrics, which include the design and deployment costs, the complexity of the technology, the usability and so on. The comparison of the techniques is based on collected evidence both from literature and from direct feedback from law enforcers and stakeholders.

The report also links the design and deployment of the identified techniques with organization and processes aspects. The feasibility and operational success of some techniques is only possible if an organization framework (e.g., supply chain management) is in place. On the other side, specific technologies (e.g., authentication technologies) can greatly improve organizational-based approach to limit the risk of distribution of counterfeit products.

The report does also present the concept of "empowerment of the consumer" where technologies for fight against counterfeiting can also be used in the field by the consumer. Here the term consumer can include citizens, law enforcers or even small companies with different capabilities and goals. The concept of "empowerment of the consumer" is based on the increasing capabilities of mobile devices and systems in term of processing power, wireless connectivity and sensor accuracy, which allows the implementation of technologies, which were confined to forensics laboratories until recently. The overview of the techniques for empowering the consumer will be the main focus of a subsequent report.

Privacy aspects are also taken in consideration. Because many techniques are based on the authentication and tracing of the "good", this information could also be used to track the individual and impact his/her privacy. The report provides some insights on the approaches, which could be used to mitigate these risks.

Finally, the report recommends actions and suggests areas where policies and practices to combat counterfeiting could be strengthened.

The following recommendations are suggested:

1. The application of Due Diligence and Responsible Supply Chain Management to e-commerce distribution should be further analysed and the definition of a suitable regulatory framework should be supported.

2. The application of techniques for forensic analysis to empower law enforcers or even the generic citizen in the field in the fight against counterfeiting should be supported in collaboration with industry and standardization bodies.

3. Standardization activities for the usage of consumer equipment like smartphones for fight against counterfeiting (including awareness) should be supported.

4. A knowledge management database should be put in place at European level. The Office for Harmonization in the Internal Market (OHIM) and Observatory could be quite suitable to this goal.

5. Regulatory frameworks or guidelines should be put in place to support brand owners in their choice of selecting the best techniques for fight against counterfeiting.

6. A cost/benefit analysis should be implemented for the deployment of authentication technology in the product design, manufacturing and distribution processes in different market sectors.

1. Introduction

The scope of this technical report is to provide an overview of the possible techniques to fight against counterfeiting. With the term "technique", we intend a technology and/or a process or both, which can be used in the fight against the production and distribution of counterfeit products.

Note that in this report, we will use the term counterfeit to include the infringing of Intellectual Property Rights (IPR).

Counterfeiting is a very wide phenomenon, which is increasing in scope and magnitude and which affects many different market sectors. Many different types of goods are impacted by the counterfeiting problem and one specific technique may not be appropriate to all the different types of goods. Each technique has also different degree of maturity. Some techniques are still very much in the research phase and used only in forensic labs while other techniques have been used for thousands of years but they are still applied with increased level of sophistication.

Note that the report only focuses on physical goods and not digital goods. In other words, piracy of digital media is not addressed in this report.

The objective of this report is to provide a comprehensive but not necessarily detailed survey of all the different techniques, which can be applied at different levels of the fight against counterfeiting: from awareness and detection by consumers, identification by law enforcers, analysis in forensic labs or organization processes and best practices.

The reason why this technical report is not focused on a specific area or phase in the overall anti-counterfeiting process is because the technological evolution has allowed the adoption of techniques previously confined to forensic labs to phases, which are nearer to the consumers. In a similar way, techniques previously used only by manufacturers and distributors are available to a larger variety of stakeholders from consumers to law enforcers.

The reason why the report may not provide a very detailed view of the specific techniques is because there is already an extensive literature for each specific technique. This report itself has been drafted on the basis on a very long list of references from public, private, research and media sources, which the reader can use to investigate more in detail a specific technique.

One important goal of this report is to provide a qualitative analysis to evaluate the different techniques regarding various metrics and different domains. This is presented in an Excel matrix in section 10.

The importance of consumer technology like a smartphone or other portable equipment to fight against counterfeiting in the field is another element of this report, which is briefly address in a section focused on the concept of "Empowering the consumer". This topic will be the main objective of a subsequent report.

There is no specific target audience of this report. The report aims to help the reader on the potential techniques, which can be used against counterfeiting at the time of writing (October 2015).

The structure of this report is following:

- Section 2 describes the main classifications of anti-counterfeiting techniques.
- Section 3 describes the main domains (market sectors) addressed in this report.
- Section 4 provides a description of the main authentication technologies, where a taxonomy has been created on the physical features of the good.
- Section 5 describes the techniques based on the concept of "track and trace"

- Section 6 describes the techniques based on container, packaging and sealing.
- Section 7 describes new trends in the counterfeiting phenomena and the related techniques to address them.
- Section 8 describes techniques based on the definition of organizational processes and structures.
- Section 9 briefly describes the main government and private initiatives for fight against counterfeiting.
- Section 10 provides the comparison matrix where all the techniques described before are qualitatively evaluated against a list of described metrics.
- Section 11 briefly describes future emergency threats in the counterfeiting context.
- Section 12 describes the concept of "empowering the consumer".
- Section 13 provides a list of recommendations and areas where actions should be taken.
- Finally section 14 provides the conclusions to the report.

Annex A.1 provides the evaluation tables of the techniques presented in this report.

2. Classification of techniques for fight against counterfeiting and IPR infringement

Counterfeiting is a longstanding problem which is growing in scope and magnitude. As described in (OECD 2008), counterfeiting is of concern to governments because of (i) the negative impact that they can have on innovation, (ii) the threat they pose to the welfare and health of the consumers and (iii) the substantial resources that they channel to criminal networks, organised crime and other groups that disrupt and corrupt society. They are of concern to business because of the impact that they have on (i)sales and licensing, (ii)brand value and firm reputation, and (iii)the ability of firms to benefit from the breakthroughs they make in developing new products. They are of concern to consumers because of the significant health and safety risks that substandard counterfeit and pirated products could pose to those who consume the items.

The term "counterfeit" has been associated to different categories of goods, which has been copies, modified or re-branded in different ways. There are various categories of counterfeit goods in different domains and a precise taxonomy for each domain is out of the scope of this report, but we will provide two examples from two market sectors, which are heavily impacted by the counterfeit problem.

Electronic products

A potential taxonomy of the different counterfeit electronic circuit products has been presented in (Guin (2013)) and it reused here.

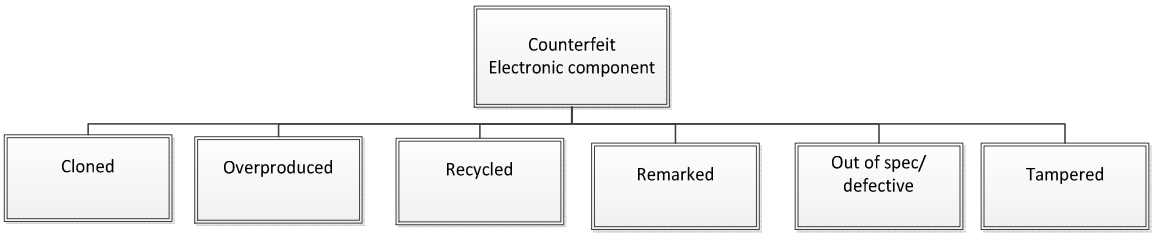

Figure 1 Taxonomy of counterfeit electronic products

Where (from (Guin (2013))), the different categories are described below:

1. **Cloned**. Cloning can be done by a) reverse engineering, and, b) by obtaining intellectual property (IP) illegally (also called IP theft).
2. **Overproduced**: Due to globalization, design houses outsource their designs for fabrication and packaging to companies all around the world, mainly to reduce the manufacturing cost. Overproduction occurs when foundries and packaging companies sell components outside of contract with the design house (component's intellectual property (IP) owner).
   Note that this category does not include overproduced goods, which have identical components and design of the valid goods. In this case, this is considered a contract policing issue. This category is related to overproduced goods, which have different components or materials (often of lower quality).
3. **Out-of-Spec/Defective**: A part is considered defective if it produces an incorrect response to post-manufacturing tests. These parts should be destroyed, downgraded, or otherwise properly disposed of. However, if they instead are sold on the open markets, either knowingly by an untrusted entity or by a third party who has stolen them, there will be an unknown increase in risk of failure.

4. **Recycled**. It refers to an electronic component that is reclaimed/recovered from a system and then modified to be misrepresented as a new component of the proper manufacturer. Recycled components can be declared counterfeit if they are not declared as such and they are instead sold as genuine/new components.
5. **Remarked**: Most legitimate components contain markings on their packages that indicate manufacturer, trademark, part number, grade, lot code, etc. If a company is remarked to indicate another model or category, it can be considered counterfeit.
6. **Tampered**. Tampered: Components that are tampered can have dangerous consequences for the systems that incorporate them for security and safety. In this case, a good can be considered counterfeit when it has been tampered to replace internal components.

Medicines

In the medicine sector, (Davison 2011) has provide the following categories of counterfeit products:

1. **Counterfeit Product in Counterfeit Packaging**, where both the packaging and its contents are entirely false and designed to deceive.
2. Re-packaging of genuine product in Counterfeit Packaging, where authentic medicines taken illegally (e.g., theft) can be re-distributed in a new and counterfeit package.
3. **Re-using genuine packaging with counterfeit ingredients**, where discarded valid packages are re-used to store counterfeit medicines or ingredients.
4. **Re-labeling of expired or withdrawn stock**, where old stock (even expired) is re-sold as new.
5. **Re-labeling of low-dose products** to indicate more expensive doses, where the medicine or the package are not counterfeit (but maybe modified or tampered) but the dosage is changed.
6. **Usage of substitute materials** where one or more ingredients of the medicine is substituted with another ingredient.

Various techniques have been developed to mitigate the risk of the products and distribution of counterfeit items in the categories shown above. The identification and description of the various techniques is provided in the rest of the report, but we can identify a number of properties which are desirable for the techniques:

1. They should be easy to apply. This means that the complexity of the deployment of the anti-counterfeit solutions should be minimal, in particular to the production of the packaging line.
2. They should difficult to imitate. This means that the anti-counterfeit information (e.g., identity or features of the good) should be resistant against replication and cloning.
3. The costs of implementation and deployment of the anti-counterfeit solution should be feasible in relation to the specific domain/market. The cost can be different among the various domains. For example, high value goods in the retail or electronics sector may justify anti-counterfeit solutions which include expensive validation or tracking equipment.
4. They should easily support the identification of the counterfeit good from the valid good. Note that the identification of a counterfeit good can be implemented by visual detection of an un-trained examiner (e.g., a generic citizen), a trained

examiner (e.g., a law enforcer) or a forensic laboratory. More details on the different phases and categories of examiners and how they can be linked are provided in another section of this report.

5. They should be accurate in the identification of the counterfeit good.
6. They should compliant with existing international (open) standards that enable interoperability of the technology for all participants in the supply chain as well as the products' end users (i.e. consumers, law enforcement agencies, experts).
7. Evidence from such technologies should be permissible in a court of law.

In line with internal market rules fostering competition and innovation, legislation should allow trademark owners (and more generally, supply chain economic operators) to select the most appropriate anti-illicit trade technologies.

More desirable features of anti-counterfeit techniques can be identified. In fact, the features identified above and other features are used in section 10. Comparison Matrix to evaluate the various anti-counterfeiting techniques presented in this report.

There are many different classifications schemes for anti-counterfeiting techniques.

One potential classification scheme/taxonomy is:

1. Anti-counterfeiting based on an electronic device added to object, which must be protected against counterfeiting. For example: RFID tag. This electronic device can be used to track and trace the object.
2. Anti-counterfeiting based on the intrinsic features of the object. For example: texture or color. This can be used to authenticate the object.
3. An additional physical element (distinct from 1), which can enhance the uniqueness of the object. For example: a label. This can be used to authenticate the object.
4. A modification which changes in a special way the intrinsic features of the object. For example a special ink or substance, which cannot be separated from the object.
5. Techniques, which are focused on the distribution channels (e.g., e-commerce) or to the correlation of data from difference elements/sources to identify anomalies in the workflow.

In this report, we will structure the survey of anti-counterfeit techniques in: a) authentication technique, b) track and trace techniques and c) other techniques including organizational approaches. Each category includes sub-categories, which will be described in detail.

As described in the rest of the report, a single technology may not be enough to address the problem of counterfeit products and it is possible that the combinations of different techniques must be used. In addition, we should consider that technologies on their own may not be able to solve the problem of counterfeiting products (Wilcok 2014). Technologies should be used in the framework of established organizations and processes within the companies and among all the stakeholders (both public and private) in a domain.

The drafting of this report is based on existing references and documents, which includes scientific papers, news report, official reports from public and private organizations and standards.

In particular, this report has adopted in most cases the concepts and definitions from standard ISO 12931:2012, Performance criteria for authentication solutions used to combat counterfeiting of material goods.

Note: In this report, the term counterfeit includes infringing of Intellectual Property Rights (IPR).

Disclaimer: In this report, case studies and anti-counterfeit products are mentioned to show the maturity of specific anti-counterfeiting technologies. It is not the intention of this report to endorse these anti-counterfeit products or the company producing them.

3. Domains

Any product can become the target for counterfeiters, particularly products or brands which are in a market leading (or second or third) position in a given country. However, to facilitate this report we here present a section which has the objective to identify the main domains where the technologies described in the other sections can be applied.

3.1. Fast Moving Consumer Goods (FMCG)

Fast-moving consumer goods or consumer packaged goods are products that are sold quickly. Examples include non-durable goods such as processed foods, soft drinks, alcoholic beverages, tobacco products, toiletries or cosmetics, non-prescription medicines, and many other consumables. In contrast, durable goods or major appliances such as electronics, mechanical, engineering, and automotive parts (and textiles to a certain extent) are generally replaced over a period of several years.

FMCG have a short shelf life, either as a result of high consumer demand or because the product deteriorates rapidly. Some FMCG, such as meat, fruits and vegetables, dairy products, and baked goods, are highly perishable. Other goods, such as pre-packaged foods, soft drinks, alcohol, tobacco, toiletries or cosmetics, medicines and cleaning products, have high turnover rates.

Although they are sold at relatively low cost compared to more durable goods, FMCG's are also substantially suffering from counterfeiting. The large quantities of FMCG sold, low public awareness re. counterfeit issues affecting FMCG's, and usually non-deterrent penalties are incentives for counterfeiters aiming at maximizing cumulative profits while minimizing risks.

The usually low margin and high volume business, the short shelf life of the items, the high speed manufacturing, the wide supply chain networks involving a high number of manufacturers, logistics service providers and distributors, and the nature of the products are important constraints to take into account when considering anti-illicit trade technologies for FMCG.

3.2. Textiles

Counterfeit goods in the textile industry have grown in recent years and the range of goods subject to infringement has increased significantly. The four most IP-infringement areas in the textile industry are:

1. High quality woven worsted with selvedge (selvedge are self-finished edges of fabric)
2. 'Noble fibres,' including cashmere
3. Interior textiles
4. Branded apparel and accessories

A detailed report on the counterfeit problem in this sector is provided in (OHIM 2013b).

3.3. Sporting Goods/Sports Equipment

This domain represents all the goods for sports activities which are not included in the textiles category. In other words, this domain includes goods like a golf club or a tennis racquet but not the tennis shoe, which is in the textiles domain. The distinction is done because of the different types of materials used in the production of the good.

A detailed report on the problem of counterfeiting in this domain is provided in (OHIM 2013).

3.4. Mechanical, Engineering, Automotive

The pressure for lower costs is one of the main drivers for IP infringers to enter the market of automotive parts. Suppliers can get a competitive advantage by offering lower quality automotive parts and components, which opens the door to IP- infringing products.

The threat of counterfeit auto parts in the automotive sector is raising growing concerns (NYTIMES (2013)). A recent recall by a major auto-manufacturer Reuters, (2014) is only one example of numerous case studies related to the presence of counterfeit auto parts in vehicles. In such circumstances, while the negative impact of an IP-infringing product can be devastating for the customer, it can also have a negative impact on the reputation of the vehicle manufacturers and lead to potential lawsuits. They also have to bear the costs of the recall of vehicles to replace the parts, which have been identified as counterfeit. By systematically applying due diligence across their supply chain automotive companies could better ensure that fewer IP-infringing product enter their market. It also includes aerospace components because of the criticality of these components and the history of fake aircraft parts causing fatal accidents.

3.5. Electronics/Integrated Circuits/Semiconductors

The infiltration of IP-infringing electronic products in the globalized supply chain is not a new phenomenon. Their level of presence in these markets has drastically increased in the last decade. This tendency has been amplified with the recycling of used components which are refurbished, but sold as new products in the market. The other main strategy of IP infringers is to re-label components to appear having a different function from their original, of course of greater value. This falsification regards both new and refurbished electronic components. This tendency may not be IP-infringing unless the refurbished components are sold under a different brand (re-branded).

In the defence market, many cases have been reported of IP-infringing or counterfeit products. The detection of such infringing parts usually occurs when there is a product or system failure, and the subsequent investigation on the root cause failure reveals that a part, or the entire product, is not authentic. However, product failures are not always easily traceable to the level of the counterfeit item. In many cases, without proper root cause analysis, the failure is attributed incorrectly to other causes. Examples of IP-infringing electronics in the defense market can be found in GIDEP, (2006) and GIDEP, (2006b).

In the battle to defend their genuine products electronics industry specialists have adopted a number of measures which are continuously adapted to new IP-infringing threats. Also innovative approaches are tested and employed to enhance the legitimate electronic products trade.

The consequences of IP-infringing components go beyond lost revenues of the electronics industries. Such components affect electronic products by degrading their performance, damaging further the reputation of the industry and reducing the market range.

Some sectors in the electronics industry can be more vulnerable to IP-infringing products than others. For example, defence hardware systems or airplanes systems are often in service for long periods, which makes them particularly susceptible to IP-infringements,

due to problems with the availability and obsolescence of parts used in such systems as described in (Stradley et al. (2006)).

A recent survey on techniques used to detect counterfeit goods is (Tehranipoor (2015)). Other references dealing with the detection of counterfeit electronic circuits are provided in the rest of the report.

3.6. Phones/Smartphones/Tablets

This category is specific to Phones/Smartphones and Table, which are a relevant market sector in counterfeit products.

3.7. Food

The problem of counterfeit food has been known for decades and it is one of the first examples of the counterfeit problem. Apart from the economic impact, safety considerations are extremely important. The range of counterfeit food products is extremely wide: from alcohol based products (e.g., wine) to meat, cheese and so on. Because of this wide range of products and because of the packaging, direct authentication of the products can be quite challenging apart from very specific types of products. Because of the complexity of the counterfeiting problem in food products, in this report, we will only consider specific categories of food with high value where counterfeit techniques have been developed. For example, wine bottles.

3.8. Healthcare

3.8.1. Medicines

The problem of counterfeit medicines is growing considerably in recent years. Ten per cent of the world's medicines are counterfeits according to the World Health Organization (WHO (2008)). The quality of the counterfeit products is usually can be so low due to the manufacturing and process conditions, that they can become a direct threat to patients' health (OECD (2008) and (Seiter (2009)). As in other domains, counterfeiting is financially rewarding and largely risk-free and terrorist groups finance their activities through the counterfeit trade and major crime syndicates are involved as well. But in this case, the safety of the people is at stake as well.

The distribution of counterfeit medicines has also increased due to the presence of numerous fraudulent websites where anyone can easily and anonymously buy prescription-only medicines as described in (Weiss (2006)). Then, a potential approach for the detection of counterfeit medicines can include both an analysis of fraudulent web sites and authentication techniques as described in the rest of this report.

3.8.2. Medical devices

Another recent development in counterfeiting is related to counterfeit medical devices. It has been reported in (Biesman (2014)) that counterfeit aesthetic medical devices have been used. As opposed to legitimate, legal devices, the counterfeit versions infringe on patent rights, falsely claim to have clearance by the US Food and Drug Administration (FDA), and infringe on branding of well recognized, FDA cleared products. In the same

source (Biesman (2014)), it has been reported that numerous patient injuries are documented to have been produced by counterfeit products. Counterfeit issues can be present for the entire medical devices or for the single electronic components used in the manufacturing process, which can make the detection of counterfeit medical devices more difficult.

We should also not ignore the new development on wearable medical devices (Gomez, (2014), where risks associated to security aspects have already been highlighted. These risks could worsen if counterfeit medical devices are used.

3.9. Agriculture

3.9.1. Agricultural products

This is a wide category, which includes different types of agricultural products including wine, oil, tobacco and other products.

3.9.2. Agrichemicals

This category includes materials used for agriculture including pesticides and fertilizers.

3.9.3. Agriculture crops and plants

This category includes materials used for agriculture crops and plants, which are protected by Intellectual Property Rights. In this case, authentication technologies are used to identify samples, which are IPR infringing.

3.10. Luxury Goods

This category includes all the luxury goods not included in the previous categories. For example, watches, jewels and others. This category is distinct from others because of lack of safety aspects, and high cost of goods, which may justify the application of more expensive techniques. An example of the problem of the distribution of counterfeit watches and the impact on the economy is provided in (WATCHES 2015), where it is reported that "Tens of millions of fake Swiss watches are offered for sale every year, while the Swiss watch industry produces around 30 million original watches. Fake watches account for 9% of customs seizures, placing watches second only to textiles as the most counterfeited products".

3.11. Paper products

This category includes paper products like banknotes, financial contracts and similar goods. This category does not include identity documents. Because these types of items are not strictly goods, they are not addressed in the analysis of this report.

4. Authentication technologies

4.1. Introduction

The concept of the application of authentication technologies to the fight against counterfeiting is quite simple. It is a classic problem of identification and authentication of an entity from another on the basis of specific features. Counterfeit goods may have some *intrinsic* or *applied* features, which makes them distinct from the valid goods. We use the word intrinsic to describe a fundamental feature of the object like the DNA of a plant or a human being. As described in the rest of the report, many objects have intrinsic features, which can be used for authentication. These intrinsic features can be the results of the production environment (e.g., manufacturing plan), the distribution environment (e.g., specific type of bacteria living on a plant after it has been planted), the composing elements (e.g., a medicine composed by specific substances or an electronic component with filters, amplifiers) or other factors (e.g. specific implementation of different algorithms in electronic devices).

To be used for authentication, the intrinsic features must have a high level of granularity as most of the authentication algorithms are based on a statistical analysis where the level of accuracy in the authentication process is related to the number of collected samples.

In the cases, where it is not possible to use the intrinsic features of the object, because the level of granularity is limited or because the intrinsic features cannot be extracted without damaging the good, additional features can be inserted to prevent clonability of the good. This can be achieved with different techniques, which are described in the report. Usually, the insertion of the additional features must be done in the production phase or the distribution phase, where the feature is applied to the object. For example, QR codes, or holograms applied to packages containing the good.

There are various classification methods of authentication technologies, which are described here.

For example, authentication technologies can be classified in two types as described in ISO 12931:2012 (ISO (2012) and (Li (2013)).

- Overt techniques, and
- Covert techniques

The main difference between the two is that overt technologies can be verified by users who are familiar with the overt technology and – for preference – have a reference genuine sample of the feature with which to compare the suspect feature on the suspect good, while covert technologies require experts with specific (e.g., laboratory) equipment to be verified, as the details of the technology are not disclosed and available to those who have administrative responsibility over the deployment of the technology. In a way covert technologies adopt an approach similar to the concept of "security by obscurity". Another difference is that (Davison 2011), overt techniques are mostly based on the sensorial capability of the human being: sight, sound, smell, touch and taste, while covert techniques are based on the digital information present in the token, which must be processed by a digital device (e.g., a computing device).

Examples of overt technologies include holograms, colour-shifting inks, security threads, watermarks and sequential product numbering. Depending on the product they can be integrated using chemical or physical markers as it happens for banknotes and documents. Special inks technologies include invisible ultra-violet (UV) inks which are visible only with ultra-violet lamps and colour-shifting inks which change colour

depending on the view angle. Watermarks and security threads (a thin ribbon of metal or plastic) are also techniques widely used for banknotes. Another overt authentication technology is fluorescent fiber which is inserted in the paper-making process.

Covert technologies include also similar elements such as security inks, digital watermarks, biological taggants, chemical or microscopic taggants. An example of covert technology used again in document security is micro-printing where complex artwork is generated made of multiple fine lines. They are difficult to replicate and counterfeited prints are easily identified by document security experts.

Another classification of authentication techniques is based on the identified part of the spectrum, where the authentication can take place: from visible light, to infrared, radio frequency emissions or analysis with high energy rays. While the complexity of authentication techniques in the visible light is usually low (e.g., simple visual inspection belongs to this category), authentication based on high energy rays (e.g., X-Ray) require expensive equipment, which requires specific training. Another set of authentication techniques is based on the electrical or chemical properties of the good.

The classification of the techniques can also be based on the phases of the evaluation of the goods. We can identify three main phases for the authentication of a good (these phases are derived from (ISO (2012)):

1. Detection based on overt features, where an examiner inspect a good on basis of the human senses and it does not require any additional equipment to allow a feature to be verified as genuine. For example, the visual inspection of a good to examine if the brand identifier (e.g., logo) is valid. A malformed logo could indicate a counterfeit good.

2. Detection based on a required authentication tools and/or specialized knowledge to verify their presence and validity of authentication elements in a good. For example, a QR code reader could support the identification of a good by checking the QR code identifier against a remote database.

3. Forensic analysis, which requires the use of knowledge and dedicated scientific methods to validate the authentication elements or intrinsic attributes of a material good. For example, a spectrometer could be used to identify the chemical elements of a medicine. A counterfeit medicine can have different elements of different percentages from a valid medicine.

Different types of stakeholders participate to different phases: while a generic consumer or a custom officer can use authentication techniques in phases 1 or 2, phase 3 is mostly adopted by forensic labs owned by a company (e.g., the brand company itself), a company specialized in forensics analysis or a government agency.

In this report, we decided to adopt the taxonomy of the authentication techniques shown in Figure 2, which is mostly based on the physical characteristics of the good. On the left are listed all the authentication technologies, which are based on the electromagnetic spectrum emissions from the good itself. They include the basic visual inspection but also very sophisticated radio frequency analysis techniques. On the right, are other authentication technologies based on chemical, acoustics and other means including the DNA of organic goods. A specific category is defined for the authentication technologies based on the artefacts produced by the good itself. This is a recent category, which is the result of the technological evolution of consumer electronic and their capabilities. For example, a smartphone can be identified by the images, which are collected by the smartphone itself as described in section 4.10. Authentication based on artefacts generated internally by the good.

Please, note that this taxonomy is defined independently of the different categories of goods and domains defined in section 3. Domains. Even if examples of the goods authentication are provided, an analysis of the feasibility of each authentication technique is provided only at the end of the section.

The description of the technique is also independent from the phase where the good is inspected. It is the objective of section 10. Comparison Matrix to evaluate the different techniques against a range of metrics. In particular, we are interested to the evolution of the technologies, which allowed some authentication technologies to move from phase 3 (Forensic analysis) to phase 2 (Detection based on a required authentication tools). This technological evolution is a key to support the concept of empowering the consumer presented in section 12. Empowering the Consumer and in a technical report subsequent to this one. In other words the advancement of technology has allowed the application of technologies and tools designed for forensic analysis to the detection phase, which can be performed by customs officers or even the generic citizen with low cost equipment or even consumer equipment like a smartphone.

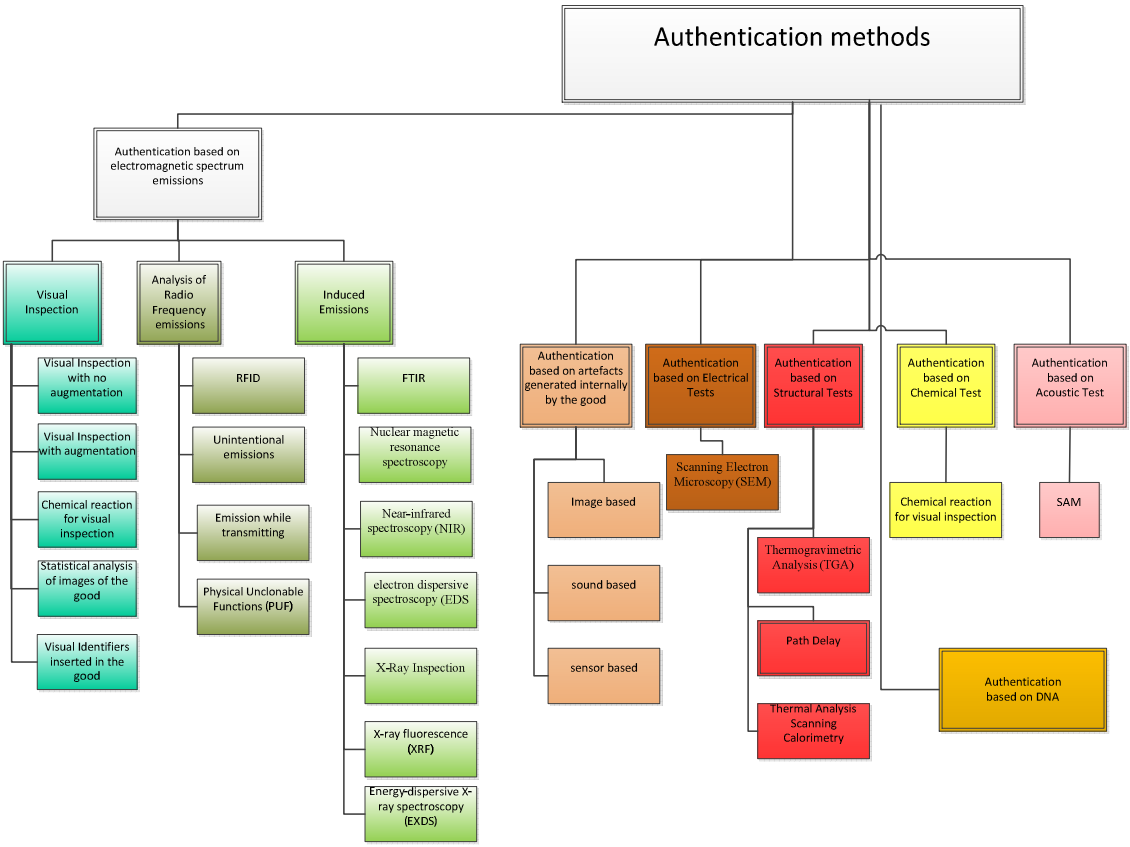

Figure 2 Taxonomy of authentication methods

4.2. Authentication based on electromagnetic spectrum emissions

The following sections describe the techniques, which can be used to authenticate a good on the basis of the electromagnetic spectrum emissions, which includes visible light (e.g., simple visual inspection of the good), radio frequency emissions (e.g., the phone when it is transmitting), infrared or others.

4.3. Visual inspection with no augmentation

4.3.1. Description of the technique

In this section, we describe the basic visual inspection technique with no added visual identifiers (e.g., holograms), which are instead described in section 4.7. Visual Identifiers inserted in the good.

Visual Inspection is the oldest and fastest technique to detect counterfeit goods. The inspectors try to identify traces of refurbishing or relabeling work done on the components. A general characteristic of the anti-counterfeit inspection methods in electronics field is that because of the size of the components, microscopes or other visual technologies (X-rays) are required (see also the following sections on the augmentation of the visual techniques).

The identification of the traces is based on acquired information about the tools and the substances used, as well as on the overall experience gained through the years in the fight against counterfeiting. Chemicals may be used when substances need to be the identified. Automated vision systems have been tried for industrialised inspection solutions, but the usual approach is to use samples, inspected visually by experts.

Counterfeit items are usually distinguished due to bad reproduction of logos, imperfections in the casing or the package or different internal features (e.g., different placement of the batteries or the circuits). On the web, there are various examples and tutorials to distinguish and identify counterfeit products from valid products. Medicines can be distinguished by the slightly different colour or by a different casings. Apparel is usually distinguished due to a low quality logo on the dress.

In the case of electronic components or mechanical items, the most common evidence searched with the visual inspection are the following features:

- sanding marks
- polymer masking (blacktopping) to cover marks
- bent leads,
- replated leads
- evidence of rework
- quality and correctness of markings and logos

A fast and easy method to identify if an electronic part has been remarked or resurfaced is to apply on the surface a chemical substance. There is a number of mineral spirits together with isopropyl alcohol which are used. If the marking is able to be removed using this solution, the component is suspect for counterfeit if the marking are easily removed.

To detect possible resurfacing or polymer blacktopping acetone is also used.

Blacktopping can also be detected using a standard blade to scrape off the polymer film.

4.3.2. Analysis of visual inspection with no augmentation

Visual inspection is currently one of the most common techniques to identify counterfeit goods and it is usually reported in various Guidelines and Best Practices for fight against counterfeiting (see for example (WHO (1999)).

The Visual inspection can be augmented by different means. The most simple is to use a loupe (magnifying glass). The application of a microscope to enhance *forensic* visual inspection in fight against counterfeiting of goods is pretty obvious but there have been recent developments in this area, which are described in 4.4. Augmented Visual inspection.

The simplest visual augmentation tools are: loupe, laser pointer, polarising filter and scrambled indicia viewing filter.

The advantage is that it can be applied to a large variety of goods and materials and the related packaging.

Another advantage is that it does not require expert knowledge in using a specific instrument (e.g., spectrometer) and a generic person could try to distinguish a counterfeit good from a proper one if he/she is made aware of the differences (e.g., counterfeit awareness web sites or other tools could provide this information to the generic consumer). This is one of the aspects of "empowering the consumer", which is described in section 12. Empowering the Consumer.

The disadvantages are:

a) that it requires specific knowledge of the counterfeit good to inspect the specific differences with the valid good. This knowledge is continuously changing due to improvements in the quality of the counterfeit models. As a consequence, an inspector (e.g., a law enforcer) can have problems in being updated on all the possible counterfeit models or new types of counterfeits.

b) The quality of counterfeit goods is improving and cosmetic or external differences may not so visible as in the past. As a consequence, it may be difficult to detect them with a naked eye as in the case of small electronic circuits or medicines. In this case other techniques, which are related to the intrinsic properties of the good must be used.

4.4. Augmented Visual inspection

4.4.1. Description of the technique

The Visual inspection can be augmented by different means. The most simple is to use a microscope.

The application of USB microscopes, which provide the image directly to a computer has been mentioned in (Villasenor (2013)) specifically for the fight against counterfeit circuits. The USB microscope is fairly inexpensive. For the detection of counterfeit parts, a microscope with at least 30X magnification is recommended. It is also important that the user have a camera built into your microscope (see (AERI (2015))).

More powerful tools have been researched and developed by DARPA as described in (DARPA (2014)). One of the contractors of DARPA has developed and deployed an Advanced Scanning Optical Microscope that can scan integrated circuits by using an extremely narrow infrared laser beam, to probe microelectronic circuits at nanometer levels, revealing information about chip construction as well as the function of circuits at the transistor level.

Beyond the microscope, other technologies like X-ray or the electron microscope can be used to effectively augment the visual inspection of a good. Because these techniques are based on the induced emissions generated by a stimulation (e.g., electronic beam), they are described more in detail in section 4.9. Induced emissions (spectroscopy, magnetic resonance and similar techniques).

4.4.2. Analysis with Augmented Visual inspection

Augmented Visual inspection is a very common method for detecting counterfeit goods. In comparison to the simple visual inspection, it requires test equipment like a microscope, which introduce an additional cost. On the other side of the coin, low cost microscopes are now available in the market, which can be connected to the computer like the USB microscope identified in (Villasenor (2013). In these cases, the inspector can also have the additional advantage that the computer connected to the USB microscope can implement algorithms for image recognition or image enhancement.

Advantages and disadvantages are quite similar to the visual inspection and we refer to 4.3. Visual inspection with no augmentation and 4.4. Augmented Visual inspection for the rest of the analysis.

4.5. Chemical reaction for visual inspection

4.5.1. Description of the technique

This technique uses a chemical reagent to distinguish between a fake or valid product. The method can be used in electronic circuit's identification as it is not destructive. For example, acetone is a common chemical to determine if the part of an electronic circuit has been remarked. A less harsh solvent can be a combination of 3 parts mineral spirits and one part alcohol. This is the mixture that MIL-STD-883 (method 2015.13) requires part markings to withstand (see (AERI (2015))).

4.5.2. Analysis of chemical reaction for visual inspection

The main disadvantage of this technique is that it requires test lab tools and materials (e.g., chemical reagents) and it requires the adequate training to use them. Even with this disadvantage, chemical reaction is used with good accuracy for the identification of counterfeit medicines (Hu (2006)) or electronics.

Another disadvantage is that the test can be destructive on the good to be identified.

The advantage is that the test bed is relatively cost-effective and the needed training is relatively simple.

4.6. Statistical analysis of images of the good (object recognition)

4.6.1. Description of the technique

The statistical analysis of images taken from an item or good can be a powerful enhancer of visual inspection. The concept of object recognition is to collect images of the good under examination or parts of the good and compare them to a reference of the valid good to understand if the good under examination is a fake or not. In other words, object recognition is the task of recognising the presence of a specific instance of an object (e.g., a specific bottle, a specific car), given one template image showing the object of interest. Object recognition is mostly a matching problem (i.e., images are compared – matched – with a template).

Unique optical intrinsic properties of the good can be used to combat counterfeiting. For example, the analysis of the image of the fabric of the textile component of a luxury bag can be used to distinguish a fake bag from a valid bag.

One can distinguish between two main categories of object representation, namely *window-based* and *part-based* models. Models of the first kind describe the object appearance *as a whole*, within a certain region of interest (the *window*); instead, models of the second kind consider objects as composed by several parts, whose appearance is described separately, and are typically accompanied by a set of geometric constraints of the location of the parts with respect to each other. While window-based models generally work well for rigid objects (e.g. a bottle), a part-based model is more suited to describe objects that have kinematics (e.g., the human body). In both cases, different features can be used for statistical analysis and object recognition as described in (Carbonetto (2004)):

1. **Colour**. The colour of the image of an object is one of the features, which can be used to identify an object even if colour alone may not be enough to identify an object. In fact, while colour can be important for recognising some categories, in practice the actual colour perceived by the machine is strongly influenced by illumination conditions, and achieving invariance to illumination is still a challenging and largely unsolved problem in computer vision. In addition, colour information alone cannot encode the object shape, which is an important and discriminant cue.
2. **Shape**. The shape of an object or part of it (e.g., the antenna of an automotive telematics component) is another feature, which can be used to identify an object. A shape-texture cue is described by an orientation histogram, which is computed based on image derivatives in x and y directions (Wang (2008)).
3. **Texture**. Image texture is defined as a function of the spatial variation of pixel intensities. A textural signature is capable of capturing inherent features, and it is usually capable of coping with various changes in the environment (e.g., change of lighting).

The basic approach to object recognition, which can be adopted in fight against counterfeiting is based on the following phases:

1. **Library** creation. Creation of a library of test images of valid goods.
2. **Features extraction**: features are extracted from the image taken of a good under evaluation.
3. **Matching**: local features from the template image(s) are compared against the ones from the library.
4. **Verification**: during the previous step, a number of wrong matches are expected to be found; an additional verification phase takes care of filtering out the mismatches, typically by checking the geometric configuration to ensure it is consistent with the layout of the template object. The output of this final step is the identification of good under evaluation as fake or valid good with a specific probability.

While object recognition is well known techniques used in many domains, there are considerable challenges, which limit its applicability in the fight against counterfeiting:

1. **Lighting conditions**. A change in the illumination conditions (intensity and colour) can heavily affect objects' appearance. Descriptors used to represent the object should be robust/invariant to such changes.

2. **Appearance changes** due to rotations, viewpoint and perspective. Depending on the position and pose of the object in the scene, its appearance may strongly vary. This problem becomes even harder in case of non-rigid objects.

3. **Occlusions**. The object of interest may be partly occluded by other objects in the scene. As a result, the appearance "perceived" by the machine changes (as it incorporates spurious elements from the objects responsible of the occlusion); this can ultimately lead to a missing detection.

4. **Availability of training data**. Learning a model of the object requires an appropriate amount of training data, i.e. images of instances of the object category to detect. Such data should in principle show the full range of appearances of the object category. It is often difficult, and a time-consuming activity, to collect and label such images. In fact, to increase the probability of finding the same object in a corpus of images and videos, one should give to the system enough examples (e.g., images showing the object of interest in front pose, in rear pose, on top, etc.) to represent the whole appearance variability. However, in typical application scenarios only one or a few examples are available, which can severely limit the practical usefulness of object recognition.

As a consequence, object recognition has many limitations for fight against counterfeiting even if it can be applied in very specific fields where the creation of the library is relatively easy and the challenges are somewhat mitigated (e.g., lighting conditions can be set).

Object recognition can be enhanced by specific features inserted in the object as described in the following section.

4.6.2. Analysis of Statistical analysis of images of the good (object recognition)

The application of images recognition for fight against counterfeiting has been widely addressed in research literature but the market deployment is limited because of the challenges described in the previous section.

In (NEC (2014)), NEC described a solution, which overcome some of the challenges described above because specific patterns are embedded in pre-identified parts of the good. As with similar techniques, the creation of a library is still required to implement the system. The NEC solution could be a precursor of similar techniques in the coming years.

The advantage of the technique is the simplicity and the cost effectiveness: only a camera and a connection with adequate bandwidth is needed. In fact, this technique is one of the candidates to implement the empowerment of the users because a generic smartphone is what is needed from the consumer side.

Note that object recognition could be enhanced by inserting visual identifiers in the good and then updating the reference library with the information on the visual identifier. The techniques based on virtual identifiers are described in the next section.

4.7. Visual Identifiers inserted in the good (Overt and Covert)

4.7.1. Introduction

The identification of good can be enhanced by using visual identifiers inserted in the good to enhance the visual inspection or the other identification techniques described previously in this report (e.g, 4.4. Augmented Visual inspection). The application of

visual identifiers applied to the good or the package is a very popular category of anti-counterfeit techniques because of its limited costs and easy of deployment. The disadvantage is the risk of cloning the identifier.

Well know methods, which already applied for the fight against counterfeiting, include (see Li (2013) and (WHO (2015))) various overt and covert technologies, which are described below.

Note that overt technologies can also be used as covert technologies and vice-versa depending on the complexity of the design. Most of the recent developments in overt and covert technologies have embedded hidden features in over technologies to make them more difficult to be cloned.

4.7.2. Overt technologies

This category includes all the techniques where the authentication artifacts applied or built into labels, documents and packages are quite visible to the user and show dynamic visual effects.

Each technique is described in detail in the following sub-sections. Note that some of these techniques can also be covert features depending on the design of the technique for fight against counterfeiting.

4.7.2.1. Holograms

Holograms, which incorporates an image with 3D or another visible construction. Holograms are three-dimensional drawings that can be used as foils, stickers, labels and films. Hologram serves as a detection feature. When sophisticated criminals have the resources to reproduce packaging that is barely distinguishable from the genuine, the same cannot be said of the fake holograms. In this category, we include only simple holograms, which are a type of the more general category of OVD described in the next bullet.

In this technique, we also include colour shifting elements or inks, where color changes are used to uniquely identify an item or type of item. Color-shifting ink changes color depending on the angle at which the package is viewed

In this technique, we also include colour shifting elements or inks, where color changes are used to uniquely identify an item or type of item. Color-shifting ink changes color depending on the angle at which the package is viewed.

There are many examples of holograms in the market available today (October 2014). Here we provide some examples, just to show that this technology is well understood and applied in the market in various domains and applications. Examples of products already available in the market are:

- (SICPA 2015), which produce security inks, which are devised to protect banknotes and security documents from the threats of counterfeiting and fraud. They range from inks developed for specific printing processes to theft-deterrence system.
- (KBA 2015), which produces special inks for the production of bank-notes (e.g., South African bank-notes). KBA-NotaSys range of equipment covers several printing processes. They includes: a) Intaglio printing, which provides the note's relief, tactility and fine lines, b) Offset printing, which is used to display multi-colour designs, c) Silk Screen printing, allowing the application of thick ink films, especially for optically variable and iridescent inks, d) Application of Optical Variable Devices, either as continuous stripes or individual patches e) Laser Marking, involving the application of laser based features and others.
- (Zeiser 2015), which uses inks together with other technologies to mitigate the risk of counterfeiting of ID cards. One of their line of products is PERSOLINE ID, which is a modular tool solution created by Atlantic Zeiser to provide full-color

personalization of ID cards. To maximize durability and security, the machine incorporates several technologies in one single solution: from laser personalization and inkjet printing, to digital UV varnishing and security lamination.

As noted in the introduction of this technical report, these examples should not be meant as recommendations by this report. These examples are just provided to show the maturity of these techniques in the market.

4.7.2.2. Optical Variable Devices (OVD)

Optically Variable Devices (OVD), where complex images or texture change image or colour depending on the angle of interaction between the viewer, the object and (sometimes) an illuminating light source. The goals is to make the OVD so simple (and cost-effective) in its visual change that it is easily remembered and recognized, but so complex in production that it cannot be easily cloned or reproduced.

There are many companies, which produce anti-counterfeiting products based on OVD. Apart from KBA-Notasys described previously, Optaglio is another company, which applies OVD in the production of banknotes and national identity documents. Optaglio has developed Nanogravure™, Banknote foils and OVDot™. Nanogravure™ indicates nano-engraved holograms developed and patented by Optaglio. OVDot™ indicates a technology developed by Optaglio using metallic holographic elements for covert marking against counterfeiting and fraud.

4.7.2.3. Watermark

This was one of the early technique to mark the surface of a good or even a digital artifact (e.g., image or movie where watermark is also called digital watermark) through a pattern, which was not obviously identifiable. Watermarks are used in banknotes often in combination with the other techniques described here. For example watermark can be implemented with special inks or holograms.

The main strength of the watermark is that the technique become an intrinsic feature of the good rather than being just applied (and then easy to remove). The disadvantage is that it can be cloned and the challenge is how to make the cloning process so difficult that it is not worth for a counterfeiter.

4.7.2.4. Security thread

Security thread is a metal thread or polyester plastic thread embedded in a specific part of the paper during paper preparation. On the thread, some specific characters or patterns may be printed to mitigate the risk of clonability. Usually, threads are embedded within the paper fiber and are invisible.

As with other techniques, the thread can be used in combination with other special paper making technologies such as watermark, special inks and so on.

Security threads are developed by many companies and they are usually applied to banknotes, Id documents or packages.

4.7.2.5. Fluorescence artifacts

Fluorescence artifacts are fluorescence materials applied on the good or inserted during the production phase. For example, fluorescence fiber anti-counterfeit paper is produced by adding colorless fluorescence fibers during the paper-making process. The fiber can be observed when a package with fluorescence fiber is placed under ultraviolet light. Other shapes can also be used.

4.7.2.6. QR Code

A QR code, which consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed using Reed–Solomon error correction until the image can be appropriately interpreted.

QR code is one of the most widely used techniques for the identification of goods and it can also used for tracking goods along the supply chain.

Because QRs codes are very easy to collect and process by a camera, QR code is also one of the techniques for empowering the consumers in the fight against counterfeiting as described in section 12. Empowering the Consumer.

The main strength of the QR code technique is its cost-effectiveness, the simplicity of creation of the QR code or its analysis by a consumer mass market device and the fact that a QR code can embed tracking information. The main disadvantage is that QR code can be easily cloned unless additional techniques are used in combination. Watermarks could be added to the QR code image or special inks or OVD could be used to create QR code. For example, the Israelian company Visualead (http://www.visualead.com/) proposes a technology where images or profile pictures are transformed to Visual QR Codes.

4.7.2.7. Nanoparticles

Application of nanoparticles to the good to enhance the identification. Nanoparticles can be used to implement some of the other techniques listed here. For example in (Zhang 2008), nanoparticles are used to implement fluorescence identification.

4.7.3. Covert technologies

4.7.3.1. Introduction

A covert feature is used to enable the brand owner or a specific category of stakeholder to identify counterfeit products. The generic citizen will not be aware of its presence nor have the means to verify it. A covert feature should not be easy to detect or copy without specialist knowledge.

Various covert technologies have been proposed:

- Micro-printing generates complex artwork that is made of multiple fine lines. The backgrounds of micro-printing products contain countless hexagons that not only come out blotchy, but also change the background color of faked items.
- A taggant is a chemical or physical marker added to the good to support its unqie identification. The more complex is the taggant (there could be taggants consisting of microscopic particles built up in many layers), the more difficult is to clone it, but it can also be more expensive or difficult to install in the good.
- Security inks which are visible only under a certain condition.

Variations or combination of the previous methods are described below. For example, (Warasart (2012)) uses a technique which is based on the generation of a verification code from the document in the form of a QR code, which is then cryptographically signed. In the generation process, the QR code is generated from the text of the document, which is then hashed, cryptographically signed with the private key of the document issuer and further compressed. The resulting QR code image is printed on the document itself. In the verification process, the reverse is done starting with the OCR processing of the printed QR code through to the validation of the digital signature.

Use of taggant markers embedded in the tear-tape of the product's wrapper (for example, polypropylene film) increases the level of security and protection of a product against counterfeit.

Taggant markers are a recognized invisible security element widely used in various industries. Taggants are specific invisible chemical markers, proven to be a highly secured technology, which can be authenticated by specific inspection devices. The taggant is embedded in the tear-tape of the product/item/packet's wrapping film. The removal of the tear-tape is an immediate sign that the product/item/packet's integrity has been tampered with: once removed, they cannot be re-applied and thus make clear that the product they secure has been tampered with.

As an example, taggant, tear tapes and cello (polypropylene film) are integral parts of products wrapped into a packaging unit. Taggant tear-tape is generally admissible in court to assist authentication.

Another way to apply a security feature - one of the latest innovations in this area - is to spray invisible substance over products. The technology is extremely difficult, if not impossible, to mimic, and relatively cost-efficient, as it is applied to the outer packaging during its manufacturing or at product packaging time.

Another techniques, which is very simple to use for the consumers is through polarized filters. A polarized filter implemented on a simple strip can be used to highlight features embedded on a material (e.g., textile) or a label. In other words, an hidden image which becomes visible only through a special polarizer. There are various examples in the market of available products using this technique like Latentogram® by ATB GROUP.

A more advanced type of taggant is proposed by (Corbellini et al., (2006)). It is based on microtaggans (microscopically traceable particles, with size from over 1 mm down to under 20 μm), realized as a multiple colour layer structure. The applicable domain is the textile industry. They are produced by a single producer who certifies and register in a database the taggans generated for each customer. In (Corbellini et al., (2006)), the authors describe their solution which is based on two-dimensional bar codes which carry information about the product such as producer name, product identifier, date and time of production that has been cryptographically signed to guarantee authenticity. The barcode is then marked directly on the textile. Issues which may raise from the particular support on which the barcode is printed are discussed. A deformation index has been studied to verify if a material is suitable for marking using the proposed technique. According to the authors, the marking system has proved to be applicable on most kinds of commercially available textiles.

The security features are designed to provide authentication, i.e. to verify immediately whether a product is genuine. One essential characteristic of a security feature is to be resistant to counterfeiting or duplication.

The method of putting the security feature on the packaging unit is also an important issue to take into account while applying technologies to protect the products against counterfeit. To ensure its effectiveness, and to be admissible in court to authenticate the product, the security feature must be part of the product's packaging.

4.7.3.2. Analysis of Visual Identifiers inserted in the good

The application of visual identifiers both overt and covert represents one the most common category of techniques for fight against counterfeiting for various reasons. Primarily they are very easy to apply to various types of goods in different domains. For example, QR codes or special inks can be used on labels of packages of food specimen or medicines or banknotes and so on. Secondly, another strong advantage is the price. Most of the overts or coverts technologies are very cost effective with a price of few cents for thousands of items. A third advantage is the simplicity of the control systems like readers, which can be just a simple camera connected to a remote server for checking the collected data against a reference library. A smartphone with an application

connected to a remote server, where the overt code is collected and analyzed has already been implemented by various companies. There are numerous implementation of these techniques. For example, the SICPATRACE system (SICPA 2015) can be applied to a large range of products including tobacco, alcoholic beverages, pharmaceuticals, as well as food and soft drinks. The system can be used both by generic consumers and by law enforcers through the SICPAMOBILE® device. In this example, the overt visible ink or QR code is used by the generic consumer to verify the authenticity of the product (e.g., a label on a bottle of wine) while invisible ink can be used by law enforcers.

Another strategy is to link different types of information from different technologies. For example, a Bar Code could be correlated to the QR code so that the cloning and re-use of only one of the codes would identify a counterfeit product.

One disadvantage of both overt or covert techniques is that they cannot be applied to all types of goods. They can be difficult to apply to specific categories of goods if they are too small (e.g., electronic circuit) or they are used in extreme environmental conditions like car engine components. Another issue is that the good inside the package is not authenticated. For example, medicines inside a package could be taken away and put in a counterfeit package. In these cases, the control of the supply chain or the distribution channels could mitigate these risks by ensuring the full traceability of the good and its content. Due Diligence practices could also be applied as described in section 8.1. Due Diligence and Supply Chain Management Responsibility to ensure the trust of the stakeholders in the supply chain and avoid this kind of risks.

4.8. Application of Radio Frequency emissions for fight against counterfeiting

4.8.1. Radio Frequency Identifier

The most common form of identification through radio frequency emissions is the RFID technology, which is already described in section for track and trace technologies. The concept is to create a Radio Frequency (RF) device, which emits a specific signal when irradiated. The device is applied to the good to be identified. Then, it is not an intrinsic characteristics of the good, but rather the consequence of a linkage of the good with the RFID device.

Variation of this technique are based on the coating of the good with metallic material or other material, which can radiate. For example, nano-rods can be applied to an electronic circuit as described in (Kuemin (2012)).

4.8.2. Unintentional Radio Frequency emissions

The technique is based on the concept that electronic circuits, when powered, emit radio frequency emissions, which are intrinsically linked to the physical structure of the circuit. Using a parallel from biology, the RF emissions can be linked to the DNA of the electronic circuit or component.

The idea is that electronic circuits and mobile devices which are counterfeit, have specific RF emissions, which distinguish them from valid equipment. This is due to the fact that low quality material (i.e., cheap substandard components) or low quality manufacturing practices are used to produce electronic equipment with lower costs than the valid equipment. This has been reported by many sources like (Telecom Digest (2014)) and NOKOMIS (2014).

There are various examples of the application of this technique from literature. For example, (Cobb (2012)) show how RF emissions can be used to uniquely identify integrated circuits. In a similar way, (Williams, (2010) has shown the specific identity

GSM phones can be detected on the basis of their RF emissions not only for different models but also for different phones within the same model (for example phones with different serial numbers).

In this specific case, we evaluate the RF emissions, when the electronic circuit is not communicating by wireless means either because it does not have the capability (e.g., no specific RF interface) or because it does not transmit at a specific moment or in a particular configuration (e.g., a phone set in airplane mode).

4.8.3. Radio Frequency Emission while transmitting

In this section, we focus on a specific categories of electronic systems: mobile devices (e.g., phones), which are transmitting in their allocated frequency bands. For example, the signal of GSM phone while it is transmitting a voice conversation has unique features related to radio frequency components like filters, amplifiers, and front-ends. An analysis of the signal can extract the intrinsic features of the GSM phone and disregards features of the signal related to the transmitted content (e.g., voice of the person). This can be achieved by removing the parts of the signal, which are content related. In a typical GSM burst, these parts are usually the ramp up and ramp down of the signal.

An example of ramp up for two different phones of the same model (e.g., Nexus phone) averaged on a large number of collected samples is shown in Figure 3. The small differences between the two signals can be used to identify a phone from another and a valid phone from a counterfeit phone.

As for other means of authentication (e.g., images), this requires the creation of a reference library of GSM signals from different phones/models. The reported accuracy from literature can be very high: from 94 to 100% depending on the type of phone (Hasse (2013)).

The same mechanism can be used for other types of phone or other wireless standards other than GSM.

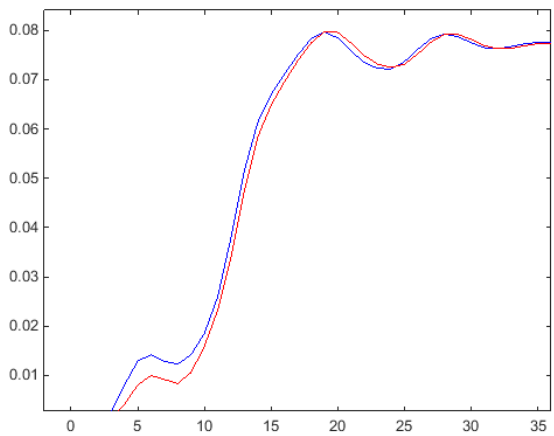

Figure 3 Ramp up of a GSM burst for two different phones of the same model

4.8.4. Physical Unclonable Functions (PUF)

A PUF can be defined as a function that is embodied in a physical structure of the good and is easy to evaluate but hard to predict. More precisely, when queried with a challenge (e.g., radio frequency emission) C, the PUF generates a response R that depends both on C and the unique physical properties of the good. For example: an Integrated Circuit can provide a specific radio frequency (RF) response when challenged by a RF emission. To be applicable for anti-counterfeit, the PUF solution must be robust,

physically unclonable, unpredictable and tamper-evident as indicated in (Tzenbeisser (2012)). Robustness is measured by similarity of the responses when the good implemented with PUF is queried multiple times. Unclonability is measured by the difficulty to create two PUFs, which are indistinguishable based on their challenge/response behavior. Unpredictability means that it should be infeasible to predict a priori a PUF response to an unknown challenge. Finally, resistance to tampering means that it should not be physically possible to change the PUFs in the good once the good is deployed in the market. In this patent proposal, we focus on strengthen the robustness and unclonability of PUFs. Please, note that PUF can also be applied to approach a) and be implemented in the devices attached to the good (e.g., RFID).

A PUF is based on the characteristics of a physical system which have the property of reacting to a challenge generating a unique response. In (Chong et al. (2008)), the authors described scattering phosphor particles as the physical identifier. The physical identifier is capable of resisting to physical cloning thanks to the random distribution of the particles. The PUF response generated from the random pattern, which is based on the phosphorescence property of phosphor particles to ultra-violet light exposure, is used to encode the digital identifier. Phosphor particles are used to generate a tag which is blended with the material used for the packaging of the product.

In addition, the authors in (Chong et al. (2008)) define the registration and verification processes which are based on the use of smartphones to take a snapshot of the printed pattern and process it to upload related information such as serial number and hash value of the digital identifier to the remote database. In the verification process, after submitting the snapshot to the remote database for verification, the user receives the results of verification via SMS. As a consequence, this technique can also be used for the empowerment of the consumer as described in section 12. Empowering the Consumer.

4.8.5. Analysis of the Application of Radio Frequency emissions for fight against counterfeiting

This class of techniques has been extensively studied in research literature where it has proven to produce very good results in term of accuracy.

The advantage of this technique is that it is based on the intrinsic features of the good rather than a label applied to it. To cheat brand-owner or law enforcers, counterfeiters would need to produce goods, with the same intrinsic or applied (e.g., PUF) features, which basically means that the counterfeiter should reproduce the same good, with no economic gain. Because low quality electronic devices usually used in counterfeit products have distinct features in comparison to the genuine products, counterfeit goods can be relatively easy to identify. In other words there is no economic incentive for a counterfeiter to build a counterfeit good with the same electronic components of the real good.

The main disadvantage of this class of techniques is the limited applicability to the category of goods, which produces spontaneous radio frequency emissions: in most cases, these are electronic components or mobile devices (even if various reports have highlighted that this is an important segment of counterfeit products). The other important disadvantage is that the evaluation of radio frequency emissions requires radio frequency test components and test benches which are usually available only in test labs. On the other side of the coin, the drop in price of radio frequency equipment has drastically reduced the overall costs of a potential test bench for radio frequency emissions and various references has demonstrated that a test-bench of roughly 1500 Euro (Hasse 2013) could be used to implement the technique described in this section. Then, this technique could be used by law enforcers to detect counterfeit electronic components and mobile devices as reported by (NOKOMIS, 2013).

4.9. Induced emissions (spectroscopy, magnetic resonance and similar techniques)

4.9.1. Introduction

This category includes authentication still based on the spectrum emission of a good but where the emission are induced. In other words, this category includes spectroscopy, magnetic resonance and similar techniques.

These technologies are usually very expensive to implement and deploy (i.e., the detection systems and test beds are very expensive) but they are used in many domains by specialized personnel. Their application to the fight against Counterfeit in the mass-market (i.e., for empowering the generic consumer of the law enforcers) is very limited at the current stage. Technology developments could change this perspective in the future. Portable systems have been reported in literature (see (Hargreaves 2008)), which implement similar functions of very expensive test bed equipment. These portable systems are described in the following sections. Apart from these portable systems, these technologies are usually adopted in the manufacturing process for high value goods or they are employed by experts in goods authentication in the private or public sector.

The following list of the detection methods and the description of physical principles that are based on is not exhaustive but includes the most frequent modern methods encountered in the literature. See also Radman (2010) for a similar survey on these technologies.

4.9.2. Nuclear magnetic resonance spectroscopy

Nuclear magnetic resonance spectroscopy or (NMR spectroscopy), is a research technique that exploits the magnetic properties of certain atomic nuclei. It determines the physical and chemical properties of atoms or the molecules in which they are contained. It relies on the phenomenon of nuclear magnetic resonance and can provide detailed information about the structure, dynamics, reaction state, and chemical environment of molecules. The intramolecular magnetic field around an atom in a molecule changes the resonance frequency, thus giving access to details of the electronic structure of a molecule. (Holzgrabe, U., & Malet-Martino, M. (2011)) apply NMR spectroscopy to the fight against counterfeiting of medicines. Equipment to execute NMR spectroscopy is very expensive and the application of this technique to the generic consumer or the law enforcer is unfeasible. Although lately small dimension experimental devices appear in the literature giving promises for hand held NMR applications, As described in (Haa (2014), NMR spectroscopy has been celebrated for its ability to probe molecular structures and dynamics with the atomic resolution and state-of-the-art NMR spectrometers use large superconducting magnets, whose high and uniform magnetic fields lead to the fine spectral resolution necessary for interrogating large molecules such as proteins. On the other side, the spectral resolution of the bulky, expensive, and high-maintenance NMR spectrometers is not necessary for a broad array of studies involving small-to-medium size molecules in chemistry, chemical engineering, and biotechnology. In this case, portable, affordable, and low-maintenance NMR spectrometers built with a permanent magnet can make the benefits of NMR spectroscopy more broadly available and enable new applications. Bulky superconducting systems have to be permanently placed in dedicated laboratories, but portable systems can enable in-field, on-demand, or online applications such as quality control, chemical reaction monitoring and counterfeiting. Still, to the knowledge of the authors of this report, there are not case studies on the applications of portable NMR spectroscopy to counterfeiting. In other words, it is still not clear is portable NMR spectrometers provide the needed level of granularity to identify counterfeit products.

4.9.3. Fourier Transform Infrared Spectroscopy (FTIR)

Another method used recently is the Fourier Transform Infrared Spectroscopy (FTIR) (Griffiths (2007)) which was developed to target organic compounds, providing an important analytical tool for characterizing and identifying organic substances. In the case of electronics it can be used to distinguish between polymers of the original cover and the polymer material used for blacktopping. FTIR can also detect other organic contaminants on a counterfeited electronic component. (Farouk et al (2011)) applied FTIR to the fight against counterfeiting of diabetic drugs.

Fourier transform spectroscopy technique shines an InfraRed (IR) beam containing simultaneously many frequencies of light in a wide spectrum. By measuring how much of that beam is absorbed by the sample material, chemical bonds and the molecular structure of organic compounds can be identified. This process is repeated many times. Afterwards, a computer takes all these data and works backwards to infer what the absorption is at each wavelength.

This provides the ability to non-destructively determine the source of organic contaminants in areas such as electrical contacts, metallization lines, magnetic disk drives and die surfaces (Shrivastava, (2014)). Recently two technological improvements in FTIR, i.e., microbeam technology and attenuated total reflectance (ATR), allow investigators to analyze thin films, organic and inorganic, in areas as small as 10-15 microns.

The application of FTIR for the detection of counterfeit Viagra has been reported in (Pereira (2014), where fifteen commercial samples (Viagra® and Cialis®) and thirty two counterfeit samples (Viagra and Cialis) were analyzed and the FTIR data was subjected to chemometric treatment via unsupervised pattern recognition methods and a supervised pattern recognition method. The reported accuracy was quite good.

The advantage of the FTIR techniques is the high selectivity and high degree of accuracy. FTIR can identify a chemical compound in a goods or even specific materials. Portable FTIR systems also started to appear in the market like the Agilent Cary 630 FTIR Spectrometer.

The disadvantage is the collection of the samples as the material to be identified must be in direct contact with the FTIR instrument and only the surface of the material can be analysed. This impose strong limitations on many goods. Another disadvantage is that FTIR systems can be quite expensive starting from thousands of dollars to tens of thousands of dollars. In addition, the identifier of the material to be tested can be hidden by other materials as in the case of medicines.

4.9.4. Near-infrared spectroscopy (NIR)

In the beginning of 20th century researchers were able to relate the character of groups of atoms within molecules as being related to specific absorptions[1]. These absorptions are the result of interactions with the fundamental vibrations of the chemical bonds associated with the atoms of the groups. Chemical bonds can be modelled as weak springs holding together two or more atoms. When energy is added these springs will vibrate more actively and when energy is added to the system then they will vibrate more energetically. NIR is a type of spectroscopy where the near-infrared region of the electromagnetic spectrum (wavelength from about 800 nm to 2500 nm) is used.

---

[1] http://www.impublications.com/content/introduction-near-infrared-nir-spectroscopy

This technique is sensitive to both the chemical and physical nature of the sample constituents and can be performed rapidly with minimal sample preparation. NIR can be used as a screening technique to detect counterfeit samples as described in (Olsen et al, 2012) and in many other sources, where NIR is applied to pharmaceutical products. The advantage of NIR in comparison to SAM and SEM is that it can be an automatic process and not strictly dependent on SMEs.

Techniques have been developed for NIR spectroscopy of microscopic sample areas for film thickness measurements, research into the optical characteristics of nanoparticles and optical coatings for the telecommunications industry.

The advantage and disadvantage of NIR are following:

The advantage is that the technique is not destructive. In other words, you do not need to damage the good to detect a counterfeit good.

The other advantage is that the technique can be quite fast. As reported in (Olsen et al, 2012) a sample can be analyzed and identified with good accuracy in less than one minute.

The disadvantage is that it is necessary to build a library of medicines and their spectral features, which can take various days. The library must also be updated every time a new medicine or variation of the medicine is created. The other disadvantage is that the test bed can be relatively costly and it requires training of the personnel executing the test.

Finally, as with other spectroscopy techniques, the technique can only be applied to a specific type of good like medicines.

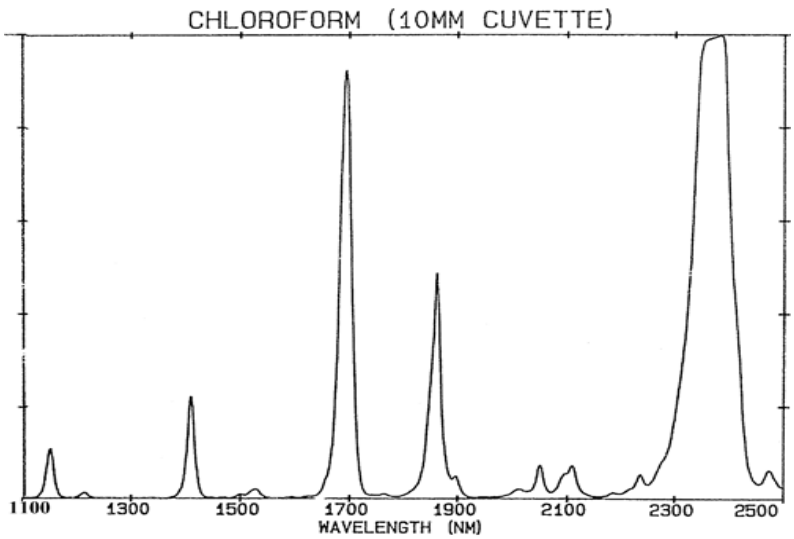

Figure 4 A typical NIR spectrum for chloroform

4.9.5. Scanning Electron Microscopy (SEM)

Scanning Electron Microscopes (SEM) were invented in 1935 but arrived at the market only in 1965. They belong to the greater category of Electron Microscopes and they use a high-energy beam of electrons to scan a sample following a raster scan pattern. The basic principle of their functioning is to collect information about the sample's surface topography, composition as well as other properties like electrical conductivity, from signals emitted from electron interaction with the atoms of the sample material.

The SEM uses the reflected electrons from the various interaction mechanisms with the sample material. This allows to SEM to operate in a number of function modes. Each mode provides different type of information about the examined sample.

The basic mode is secondary electron imaging or SEI, where inelastic electron scattering caused by the interaction between the sample's electrons and the incident electrons results in the emission of low-energy electrons from near the sample's surface.

In SEI mode, SEM can produce very high-resolution images of a sample surface, revealing details less than 1 nm in size. Due to the very narrow electron beam, SEM micrographs have a large depth of field yielding a characteristic three-dimensional appearance useful for understanding the surface structure of a sample.

A wide range of magnifications is possible. These can range from nearly 10 times (equivalent to that of a powerful hand-held lens) to more than 500,000 times, which is about 250 times the magnification limit of the best light microscopes available on the market today.

Consequently using SEM in the fight against counterfeit electronic products is self-evident since it can provide signs and traces of alterations in microscopic level. SEM can be conducted on IC or parts of electronic components after removing the encapsulates (decapsulation) or after delidding (see (Sood et al (2011)).

For example, SEM microscopy can be used to verify the elemental composition of the metallization layers. SEM can also be used to verify the solder plating composition on the part termination. In certain cases, SEM can also be used for inspecting external part packaging for signs of sand blasting and for detecting topographical changes resulting from the black-topping process. In summary these techniques are augmentation of visual inspection and they are dependent on the experience and quality of SEMs. The capability of SEM to provide magnified and detailed images from the device external or internal surfaces revealing signs that may not even be visible to the counterfeiters during the alteration process. Usually the rendered images from the inspected sample are compared side to side to images from original pieces.

One of the most common SEM uses is as a technique to detect subtle differences of blacktopping. It is impossible for blacktopping to match the exact surface texture of the original component body; SEM offers examination at several 1000x magnification in order to reveal these textural differences. blacktopping and the actual component body. Additionally, in a counterfeit goods, specific parts are handled more and go through a variety of procedures during the counterfeiting process. Each of these procedures, increases the potential of contamination of the counterfeited part. SEM can detect and identify these elemental contaminants that would not be present on an authentic part.

The advantage of SEM microscopy is that it can be used for a large variety of goods where visual magnification is used to detect counterfeit goods. Another advantage is that it does not require the a-priori building of a library.

The main disadvantage is clearly the cost. A SEM microscopy costs from ten of thousands of Euro and upwards, with precise SEM system costing hundreds thousands of Euros. This is clearly not practical for market deployment of anti-counterfeiting systems.

4.9.6. Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)

SEM and EDS, can be conducted on IC or parts of electronic components after removing the encapsulants (decapsulation) or after delidding (see (Sood et al (2011)). For example, the combination of SEM and EDS can be used to verify the elemental composition of the metallization layers. SEM/EDS can also be used to verify the solder plating composition on the part termination. In certain cases, SEM/EDS can also be used for inspecting external part packaging for signs of sand blasting and for detecting topographical changes resulting from the black-topping process. As in SAM, these

techniques are augmentation of visual inspection and they are dependent on the experience and quality of the experts.

Advantage and disadvantages are similar to SEM with an increased level of accuracy.

The disadvantage of SEM/EDS is similar to SEM already described: the cost of the test equipment is very high and in this case, the additional cost of the EDS system as well.

4.9.7. X-Ray Inspection

Known from medical applications and from security controls (e.g., airports) X-Ray inspection provides another way to obtain images of the internal structure of electronic components in a nondestructive way. Usually image magnification is applied in a simultaneously, hence it is called also X-ray microscopy. Modern X-Ray systems provide resolution of a decimal fraction of mm, and magnification of up to 10,000.

The image of the inner parts of a potential counterfeit sample is compared to the image of a certified original electronic part, from top view (but also side view may be required). This process may be done in real-time, in which case the dose rate should be taken into account.

Indeed one of the main applications of X-ray inspection is for the detection of counterfeit electronic circuits, as the very high magnification can show features like inconsistent die size, inconsistent leadframe, or broken wire bonds. In all these cases, the imperfections or differences in counterfeit circuits from proper circuits are highlighted through the X-ray inspection.

A high quality image of the internal structure of an electronic component can provide a lot of information about its intended use but also about internal alterations, defects, and degradation. X-ray flashing provides images based on material density that allow pinpointing of soldering and wire bond flaws. In addition, X-ray microscopy can reveal anomalies such as “die” attach voiding, solder pooling, or die shifting.

Some advanced X-ray systems have capabilities to perform both 2D and 3D scanning inspection. In many cases X-ray imaging operates together with scanning acoustic microscopy (SAM) since the information they provide is complementary.

The advantage is the high level of accuracy in detecting some categories of counterfeit goods. The disadvantage is the high cost of the test bed equipment and the need for training by the expert, who uses X-ray to identify the counterfeit good.

4.9.8. X-ray fluorescence

X-ray fluorescence (XRF) spectroscopy is used if more information is needed about the micro structure of the component. X-rays are used to bombard a material and then analyse the emitted "secondary" (or fluorescent) rays that return from it. This method is widely used for elemental and chemical analysis, particularly in the investigation of metals, glass and ceramics materials, and for research in forensic science, geoscience etc.

X-Ray fluorescence has been used to fingerprint medicines and distinguish valid medicines from counterfeiting medicines in (Ortiz (2012)) among other examples. As described in (Ortiz (2012), X-ray fluorescence (XRF) is a suitable technique for characterization of the presence of metals and this technique has advantageous features like multielemental capability, good detectivity, high precision, short analysis times, and is nondestructive, which makes it suitable to be extended to a great variety of samples. In case of medicines XRF presents an excellent analytical methodology for determination of active ingredient (in case of sildenafil citrate that presents sulfur, S, in its structure), excipients and covering agents as calcium phosphate, titanium oxide and iron oxide (P, Ca, Ti and Fe) that can be detected directly by XRF on the surface of pharmaceutical formulations.

The level of accuracy is quite good. The disadvantages are similar to the previous techniques: high costs of the test bed equipment and needed training of the personnel conducting the tests.

4.9.9. Energy-dispersive X-ray spectroscopy

Energy-dispersive X-ray spectroscopy (EXDS) is an analytical technique used for the elemental analysis or chemical characterization of a sample.

Analysis of the X-ray emission spectrum produces qualitative results about elemental composition of the specimen. Comparison of spectrum of the specimen with spectra of standards of known composition produces quantitative results. When an electron from the inner shell of an atom is excited by the energy of a photon, it moves to a higher energy level. The difference in energy is emitted as a photon which has a wavelength that is characteristic for the element. The presence of metal and their concentration in a good can be identified and calculated using EXDS. On the basis of the different concentrations of metals, a valid good can be discriminated against a counterfeit good.

The application of Energy-dispersive X-ray spectroscopy to detect different categories of counterfeit goods has been demonstrated by various research activities. In (Li (2011), the technique has been applied to the identification of counterfeit food. Other examples are provided for the detection of bank notes.

The advantage if the high level of accuracy.

The disadvantages are that the technique is only applicable to specific type of goods where the chemical composition (e.g., presence of metals) can be exploited for the authentication of the good. The other disadvantage is the high cost of the test bed equipment and the need for training of the tester.

4.9.10. Analysis on Induced emissions

The different techniques described in this section have some common advantages and disadvantages for the detection of counterfeit goods. The main disadvantage is the cost of the test equipment with can run from thousands of euros to hundreds of thousands of euros. The other disadvantage is that the tester must be trained to use the test bed equipment. The advantages are the high level of accuracy reported in literature to identify extensive categories of goods from medicines to food to electronic circuits and bank notes. Not all the techniques can be used for the identification of different types of goods because some technique provides visual augmentation while others are based on the identification of chemical components in the good.

An advantage of these techniques is that they are not destructive: in other words, you do not need to damage the good to identify and distinguish the proper good from the counterfeit one.

4.10. Authentication based on artefacts generated internally by the good

This section describes techniques where the authentication of the good can be done on the basis of digital samples taken by the good itself, which (in most cases) must be an electronic device (e.g., a camera) or component. An obvious challenge is that the data must be extracted from the device itself, but from an operational point of view, this can be quite simple. For example a law enforcer can take a picture from a “suspect” phone using a test SIM and compare it to a reference library of phones of the same model to confirm that the “suspect” phone is counterfeit.

4.10.2. Statistical analysis of images produced by the good

Identification of counterfeit devices with image acquisition capability (digital cameras, smartphones, tablets, webcams, camcorder…) can be achieved by characterising the image artefacts caused by the CMOS sensor (Filler (2008)) and/or by any of the post-processing steps (de-mosaicing filter (Bayram (2005)), JPEG compression (Kay (2006)), etc).

The detection of a counterfeited device can be easily performed in smartphones and tablets by different means:

1. using an application, which can to be installed in the smartphone, that analyses a photo taken using the device, and compares the artefacts found in the image to a reference library.
2. Collecting an image of series of images (e.g., around 5) and sending them to a remote application service when the image and the model is compared against a reference library.

The target for collecting the image could be a neutral background. For example, it could be a blank sheet of paper.

It is worth to point out that a database of reference artefacts should be made available and maintained, ideally populated with the cooperation of manufacturers of camera of smartphones.

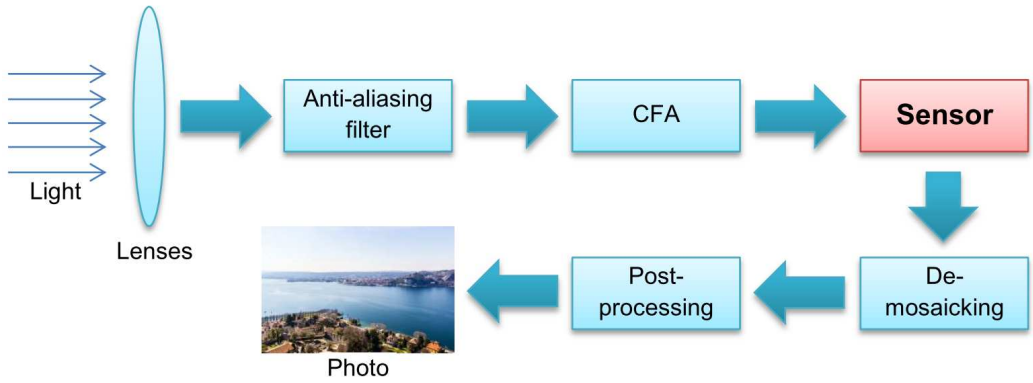

Figure 5 Image acquisition pipeline in a typical imaging device

4.10.3. Statistical analysis of audio samples produced by the good

This technique is similar to the identification of counterfeit devices with image acquisition capability described before, but it is applied to audio samples instead of images.

Detection of counterfeit devices with audio acquisition capability (smartphones, tables, webcams, camcorders, cordless phones…) can be achieved by analysing the response of the audio circuit to a standard stimulus (e.g., a standard tone). Some work has been already done in this direction in the context of digital forensics (Aggarwal (2014)) and (Romero (2014)). Cues to analyse to the purpose at hand include: microphone frequency response; effects of custom oscillators; effects produced by the Analog-to-Digital Converters.

In principle, the response of any sensor of an electronic device can be exploited to detect whether it is a genuine or a counterfeited good. E.g. in the case of smartphones, the

response of accelerometers, gyroscopes, temperature sensors, etc. This will be described in the next section.

The idea is to identify the acquisition device by assuming that the device along with its associated signal processing chain leaves behind 'intrinsic traces' in the speech signal. Indeed, the various devices (e.g. telephone handsets, cell-phones) do not have exactly the same frequency response because of the tolerance in the nominal values of the electronic components and the different designs employed by the various manufacturers as described in (Kotropoulos (2014)). Then, the recorded speech can be used to identify the device itself: if it is counterfeit or not.

4.10.4. Statistical analysis of sensor based data produced by the good

In a similar fashion of the previous methods, the identification of a device on the basis of the data collected by it, could be extended to other sensors. Sensors can be of different kind, but an important requirement is that the data collected by the sensors and used for the device identification has enough granularity to perform the identification. This means that some sensors may not be used for authentication purposes. For example, a temperature sensors or a gravity sensor may not be adapt to this purpose. Example of sensors, which can be used to authenticate a mobile device include accelerometers or gyroscopes (as reported in (Dey (2013)).

An example of the differences in the accelerometers of different smarthphones, which can be used to distinguish between valid and counterfeit smartphones is provided in Figure 6. The graph shows the different sets of collected data against time for three different smartphones of the same model when they are subject to a reproducible movement pattern. Differences in the patterns (like in the red graph from the green graph) can be used to distinguish the smartphones.

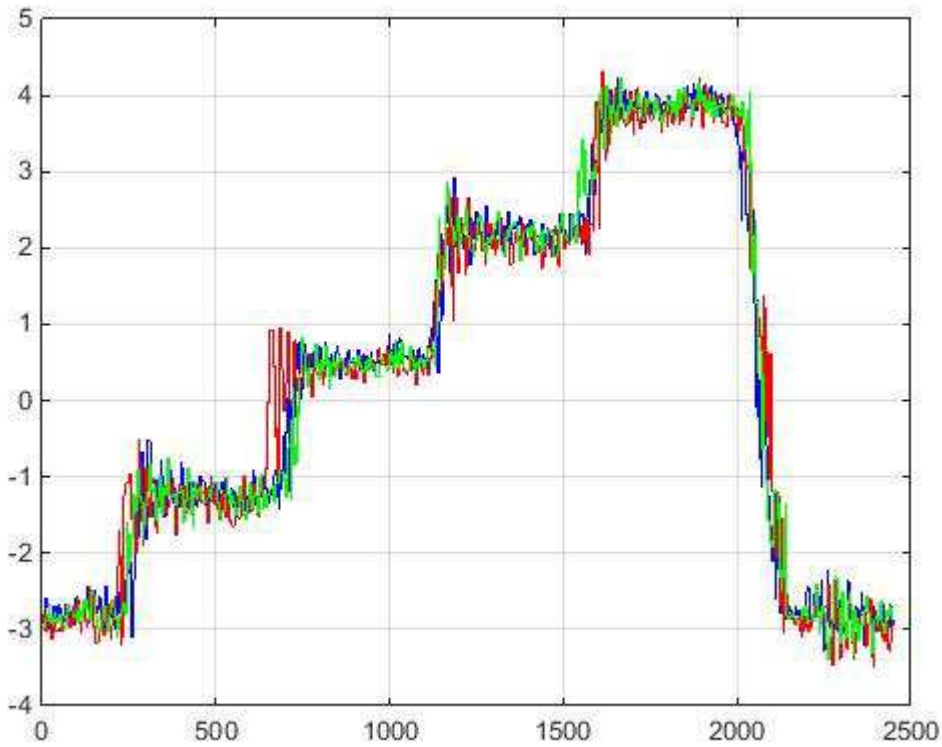

Figure 6 Differences between accelerometer data collected by Smartphones

4.10.5. Analysis of Authentication based on artefacts generated internally by the good

The techniques described above mostly originated from research efforts in recent years. The degree of accuracy can be quite high as reported by (Filler (2008)). On the other side, no products have been recorded at this moment, which are based on these techniques. Still, it is relatively easy to collect the artefacts from a mobile device and use them to distinguish a valid phone from a counterfeit phone.

The advantage of these techniques in comparison to other techniques is that there is no need of expensive equipment to distinguish a counterfeit phone from another but just the construction of a library of trained data (which can be generated by the manufacturer of the phone or the electronic device) and the definition of the validation procedure (e.g., for example take the pictures of a sample). The additional advantage is that the identification is based on the intrinsic and internal features of the electronic device, which cannot be easily faked because the economic gains in building counterfeit electronic devices in using components of inferior quality, which will be identified in the analysis.

The main disadvantage is that these techniques are only applicable to very specific categories of goods like cameras, smartphones, and any other electronic or mechanical devices, which include a sensor. On the other side of the coin, this category of device represents a very substantial market impacted by counterfeit products. As a consequence, cost effective and accurate techniques like the one presented in this section can be quite helpful to law enforcers.

4.11. Electrical Inspection

4.11.1. Description of the technique

Another approach used to detected counterfeit electronic components is to check the electric and electronic properties of the components. The level of inspection can vary from simple to a full function. The cost of the chosen inspection and the criticality of the component are two main factors to determine the level of testing. Simple inspection targets basic electrical characteristics such as resistance, capacitance, voltage or pin-to-pin values. On the other end, a full electrical/electronic inspection includes a black box approach where all the intended functions are checked using input-output measurements. Most of the times, these tests are done with the use of software, and can even include environmental factors like temperatures.

As described in (Guin (2014)), there can be (at least) four different techniques for the application of electric inspection to fight against counterfeiting:

1. **Parametric tests**,

In the parametric tests, direct current (dc) and alternating current (ac) parameters are verified. Parametric tests can be performed over a range of operating temperatures to measure DC and AC parameters of a chip. They include curve tracing test, contact test, power consumption test, output short current test, output drive current test, threshold test, rise and fall time tests, setup, hold and release time tests, propagation delay tests, etc. The objective of parametric testing is to determine the quality of each product to avoid counterfeit distribution and production. This is accomplished by running a suite of tests or as many vital tests as possible to check the DC, AC, and parametric performance of the component in question. The intricacies of these tests can easily give test engineers a robust data set that they can use to uncover a counterfeit component where other test methodologies fail to uncover any problems or anomalies (from Guin (2014)).Electrical tests require training of the personnel responsible to conduct the tests

and it also requires a dedicated lab, which could be a disadvantage in the detection phase and limits the application of this technique to forensics labs.

2. **Functional Tests**

Functional tests are the most efficient way of verifying the functionality of a component and are perhaps one of the most expensive test methods available to identify counterfeit device, which have an high degree of complexity. For instance, system memory chips will have to pass a series of functional tests exercising address, data lines, and bursting under various operating conditions (e.g., temperature, voltage, clock speed). A functional test could verify that all parts perform at specified higher frequencies and through the required temperature range using a functional baseline test (from Guin (2014)).

This type of tests usually require highly trained personnel and a complex test bench, which is also tailored to the type of electronic device to be tested.

3. **Burn-in Tests**

In burn-in tests, the component is operated at stressed conditions, such as elevated temperature, to determine failures or to highlight an abnormal behaviour. The problem of this type of tests is that they are destructive or anyway damaging the good under inspection. They also require specific knowledge of the electronic device or circuits as different devices can have different behaviour depending on their design.

4. **Structural tests**

In structural tests, test patterns are applied to an electronic device to analyse defects and anomalies related to internal structures or interconnection. The problem of this type of tests is that they requires a specific knowledge of the electronic device or circuits to compare the blueprint of the valid electronic device with the counterfeit one.

Decapsulation is also used. By the term *decapsulation* is meant the removal of the external part of the electronic component to leave the internal part exposed for inspection. Most of the times, the decapsulation results in the destruction of the electronic component. To succeed in this technique, the inspectors use mechanical or chemical tools to remove the cover or top layers of the component. Chemical decapsulation is primarily performed on plastic encapsulated components and is accomplished by applying acids onto the surface of the component to dissolving the plastic. Mechanical decapsulation is done with some tool (cutters, blades, tweezers etc.). After the decapsulation the components are investigated for the part numbers, date codes, die markings etc.

4.11.2. Analysis of Electrical Inspection

Electrical inspection has been extensively used to detect counterfeit electronic devices and it can be quite accurate when the design and production of the counterfeit device was of low quality. In these cases, the low quality of the device is revealed by the functional, parametric or stress tests. This technique is less accurate in the case of overproduced electronic devices (e.g., devices produced by the same manufacturing plant of the valid device), because the circuit design is basically the same even if the quality of the material could be worst. In this case, stress test could identify the overproduced devices.

The main advantage of electric inspection is that the producer of the type of electronic device, which is counterfeit, can easily test a counterfeit devices using the same test equipment already used for their own devices.

The main disadvantage is that the test bed setup can be quite expensive, it requires extensive training by the personnel and it can be quite specific for the type of device. In other words, electrical inspection may not be very effective for law enforcers in the detection phase, but it is mostly used in forensic labs at the time of writing this report.

The other disadvantage is that these techniques are only applicable to electronic or electro-mechanical devices, which is still a large market impacted by the counterfeit products.

Finally, we note that burn-it tests or decapsulation are destructive tests, which can also be a disadvantage.

4.12. Chemical Inspection

4.12.1. Description of the technique

The technique of chemical inspection is use a chemical agent to support the identification of the good. Depending on the type of the good, there are various chemical agents, which can be used and different processes, which can be executed.

Chemical inspection is based on the application of a chemical reagent to the good or the surface of the good or parts of the good, which reacts in different ways if the good is counterfeit or not.

Chemical inspection can be used in combination with other techniques like the visual inspection of spectrometry.

Chemical inspection is often used in the identification of counterfeit medicines as presented in (Hu (2006)), which describes the development and application of a "Fast Drug Identification System" which includes a fast chemical identification system equipped in a mobile vehicle is being developed in China and gradually put into use from 2005. Common chemical agents described in (Hu (2006)) are Sulfuric acid or Permanganate acid.

Another area is the detection of counterfeit electronic circuits and components.

The potential issue with chemical agents is that they are potentially destructive, which means that the sample could be degraded and destroyed as part of the test.

4.12.2. Analysis of Chemical Inspection

The advantage of this techniques is that it does not require complex test bed facilities as it is mostly based on the application of a chemical reagent, which can be prepared up-front. The other advantage of the technique is that it can be applied to a wide range of physical goods (e.g., medicines and electronic components). In addition, the technique can be used in combination with other techniques like visual inspection.

The disadvantages are:

a) Chemical agents can be potentially destructive, which means that the sample could be degraded and destroyed as part of the test.

b) The tester must be trained to the use of chemical reagents and in the identification of the reaction to distinguish between a valid good or a counterfeit good. Because there can be a wide range of products, this disadvantage can be addressed through detailed manuals.

4.13. Authentication based on Weight and Structural Tests

4.13.1. Thermogravimetric Analysis (TGA)

4.13.1.1. Description of the technique

Thermogravimetric Analysis (TGA), measures weight loss as a result of a variance in the temperature, which is applied to the good. This method is based on the fact that different materials (e.g., polymers) decompose losing weight at different temperatures keeping other conditions constant. Thermogravimetry is one of the oldest thermal analytical procedures and has been used extensively in the study of polymeric.

Thermogravimetric analysis (TGA) relies on the measurements of three parameters, which must be collected with an high degree of precision: mass change, temperature, and temperature change. Therefore, the basic instrumental requirements for TGA are a precision balance with a pan loaded with the sample, and a programmable furnace. The furnace can be programmed either for a constant heating rate, or for heating to acquire a constant mass loss with time.

The TGA apparatus can quantify changes like loss of water, loss of solvent, loss of plasticizer, decarboxylation, pyrolysis, oxidation, decomposition, weight % filler, amount of metallic catalytic residue remaining on carbon nanotubes, and weight % ash. All these material loss measurements are usually done during heating, but in certain cases measurements are recorded during cooling too.

Apart from the stoichiometric analysis regarding certain compounds in the material of the sample, structural defects may also become evident. The results from thermogravimetric analysis are presented (Westenberger et al (2005)) by (1) mass versus temperature (or time) curve, referred to as the thermogravimetric curve, or (2) rate of mass loss versus temperature curve, referred to as the differential thermogravimetric curve. A typical scanning rate is 10 °C/minute and information is extracted by comparing the characteristics of the curves with reference data. For counterfeit detection, TGA is targeting mainly at blacktopping and the altered polymers used for that. Comparing with original parts can reveal the differences in the material.

In the automotive sector, the application of TGA to detect counterfeit goods has been described in the test standard SAE (2015), where the test method provides the capabilities, limitations, and suggested possible applications of TGA as it pertains to the detection of counterfeit electronic components.

4.13.1.2. Analysis of Thermogravimetric Analysis (TGA)

The main advantage is that thermogravimetric analysis can be quite accurate but it is mostly based on sophisticated test bed equipment (the TGA equipment), which can be quite expensive and it require extensive training for its usage. As a consequence, this technique is mostly used in forensics labs at the time of writing this report. An additional disadvantage is that it is a destructive test as the good is subject to mass or temperature change.

4.13.2. Path Delay in electronic circuits

4.13.2.1. Description of the technique

The analysis of the path delay (Zhang (2008)) can show structural differences in electronic circuits and it can be used to distinguish a circuit from another. When an electronic circuit is used in the field, aging or environment effects (e.g., heat and humidity) could cause some of its parameters to shift over time. Similar differences can also be generated by differences in manufacturing plants and processes of different materials used in manufacturing. The test is based on the execution of a typical

workload (e.g., execution of an algorithm) a number of times. The statistical data is then collected and analysed to see the differences. The method has been proven in (Zhang (2008)) to reach very high accuracy (98-100%). Challenges are related to the cause of the differences due to aging or environmental effects, which may pose the question if the electronic circuit is counterfeit or just aged.

The application of path delay has also been reported in (Guin 2014), which also describes the main steps to be executed on an Integrated Circuit. In the first step, paths are simulated and selected according to their aging rate. Then, the delay of these paths is measured by a clock sweeping technique in new ICs (either during manufacturing test on all ICs or during authentication on a sample of new ICs) and in any available devices under authentication.

Statistical analysis is used to decide whether the device under authentication is a recycled IC. This require the creation of a library of valid ICs created at the end of the manufacturing process. (Guin 2014) reports that the used ICs can be completely separated from the signature of the new ICs, implying a 100% detection rate for recycled ICs.

4.13.2.2. Analysis of path delay in electronic circuits

Path delay is a powerful techniques to identify counterfeit electronic circuits with a high degree of accuracy and this is the strongest advantage. An additional advantage is that it is not a destructive type of test.

The disadvantages are:

1. The technique is limited to electronic circuits, which have a path for the transmission of electronic signals. Other types of goods do not take advantage of this technique.
2. The technique requires experience and training on the usage of test equipment, which can be quite specific and limits the application of this technique to forensics lab.
3. The technique requires access to the electronic circuits. While the technique itself is not destructive of the electronic circuits it may require the removal or destruction of the case of equipment where it is installed.

4.13.3. Thermal Analysis Scanning Calorimetry

4.13.3.1. Description of the technique

Recently, several thermal analysis techniques are employed in the fight against counterfeiting. One of the techniques, called Differential Scanning Calorimetry (DSC), measures the parameters of chemical reactions as a function of temperature. To perform DSC analysis, the temperature is controlled in a way that the apparatus containing the tested sample increases linearly its temperature, as a function of time. The reference sample should have a well-defined heat capacity over the range of temperatures to be scanned. The thermal analysis techniques are based on the principle that the sample (when heated) is subject to physical transformation e.g. phase transitions, while measuring the heat energy absorbed by it need to flow to it than the reference to maintain both at the same temperature.

The differences in the heat absorption with respect to a reference sample provide the necessary information to distinguish between a valid good and a counterfeit one. Parameters can be melting point, phase transition temperature, heat capacity etc. that characterize polymers used in counterfeit electronics. DSC can detect the presence of a different substance in an altered component compared to a genuine sample.

The usual operating procedure is that a sample (e.g., a medicine) and an inert reference are heated separately by two heaters at a predefined rate (measured in °C/min). A computer control, connected to sample and reference, assures that the two pans remain at the same temperature throughout the entire experiment. When the sample reaches the temperature at which it undergoes some thermal transition, its heater will have to put out an amount of heat that is different from the one of the reference. This difference in heat is measured and reported in a plot: this means that there will be a specific signal for each thermal transition.

In addition to the thermal transition, other polymorphic transitions like changes its crystalline structure or loss of water or chemical components can be detected by the DSC technique.

Beyond medicines, DSC has also been used in the detection of counterfeit electronic circuits as reported in (Sood 2011). DSC can provide clues to levels of cure of the molding compound and the numbers and types of past thermal exposures (e.g., from reworking, reballing).

4.13.3.2. Analysis of Thermal Analysis Scanning Calorimetry

The advantage of this technique is that it is quite accurate and it is based on the intrinsic properties of the good under testing (e.g., its chemical composition), then it is quite difficult to create a counterfeit item with exactly the same components of the valid good.

The disadvantages are:

1. A library of reference substances must be created. The challenge is that the analysis of all the reference substances must be conducted in the same operative conditions that will be used in the screening of the counterfeits. For example, the same kind of pan and the same temperature scan speed.
2. The technique is only applicable to goods where the chemical composition can be used to differentiate between a valid and counterfeit good.
3. DSC test beds can be quite expensive and they require extensive training. As a consequence, this technique is mostly used in forensics labs at the time of writing this report.

4.14. Authentication based on DNA

4.14.1. Description of the technique

This technique is based on the DNA analysis of organic material like an agricultural crop or plant as the DNA is unique. An example of the application of DNA checking for plants or crops is provided by (Naktuinbouw (2015)), where DNA identification is used not only to distinguish between crops protected from IPR and counterfeit but also on the area of provenance of the crops on the basis of the resident bacteria.

Another example of DNA analysis is provided in (IEEE (2012)) where DNA samples are applied to the package (in a similar way of an RFID) to uniquely authenticate the package.

Some companies have already proposed anti-counterfeiting products based on synthetic DNA sequences, which can encode company and product-specific information into inks or resins. The goal is to mitigate the risk of cloning the token or tag applied to the good.

One example is DNATech (2015), which applies synthetic DNA to covert tokens like security threats.

Another example is ADNA (2015), which instead use plant (natural) DNA to generate QR codes, which are used both for authentication and for tracking and tracing applications. The generated DNA embeds a unique serial code number, which is not easy to clone because it is part of a very complex DNA structure.

4.14.2. Analysis on Authentication based on DNA

The application of DNA (either synthetic or natural) to the production of token or tags was a technique not mature from the market point of view (i.e., still in the research phase) until few years ago. The evolution of the technology has allowed the application of this technology to fight against counterfeiting as proven by the various companies proposing DNA based products.

Because the DNA generation can be applied to covert tokens and tags, the main costs are in the generation of the token itself as the cost of covert tokens are well understood. From this point of view, this technique can be applied today to the detection phase (described in the Introduction of this report) as the information extracted from the covert token or tag through a reader can be validated against a central database.

Instead, the detection of DNA from natural samples like plants or other agricultural products is still very much (at this moment) a forensic activity to be conducted in the laboratory.

4.15. Authentication based on Acoustics tests - Scanning Acoustic Microscopy (SAM)

4.15.1. Description of the technique

Scanning acoustic microscopy (SAM) is one of the most efficient, though expensive, ways of studying the structure of a component. Scanning Acoustic Microscopy (SAM) is using ultrasound to detect possible irregularities in a suspect electronic component and is a non-destructive method (Guin 2013). SAM uses sound waves to determine density differences within a sample both external and internal. In other words, this technique functions by using the reflection or the transmission of ultrasound waves to generate an image of the component based on its acoustic impedance at various depths. For example, this is very useful in detecting delamination. When focused on the surface, SAM can show evidence of relabeling and, when compared to a known good component, it can show differences in surface texture indicative of blacktopping. Deeper in the structure of the examined good, SAM can indicate possible prior use and reworking by locating potential irregularities hinting at rework such as cracking, voiding and delamination.

As mentioned above, SAM is highly sensitive particularly to the presence of delaminations, and can detect delaminations of sub-micron thickness, which are difficult to detect using X-ray radiography. This is why the two methods are used in a complementary way. In addition to that, SAM is an important tool for detecting popcorn cracking/delamination, die attach voiding, evaluating flip chip underfill integrity, and lid seal integrity in hermetically sealed packages. Also ceramic direct bond substrates may be inspected for delamination using SAM. In addition, this technique can be used to determine the thickness of an internal layer of material.

Both delamination/cracking and die attach voiding are assembly related defects that can increase the susceptibility of components to failure in storage or use, although they may not constitute failures by themselves. Although delamination and cracking can result in sheared or lifted wire bonds, passivation cracking, metallization shifting, intermittent

electrical failures and metallization/bond pad corrosion. Die attach voiding can lead to die cracking, die attach fracture, or thermal runaway due to poor heat dissipation through the die attach.

Because SAM is basically an augmented visual inspection system, the experience and ability of Subject Matter Experts (SMEs) is essential in the identification of a counterfeit product and this factor can impact the accuracy of the overall process. As reported in (Cassell (2012)) some validation facilities and the SMEs provided different evaluations of counterfeit Integrated Circuits (IC). Some SMEs did not identify counterfeit ICs.

Currently Scanning Acoustic Microscope systems employ more data gates to easily mark delaminations and provide a wide range of transducer frequencies, from 5 to 250 MHz, to increase the effectiveness

4.14.2. Analysis on the Authentication based on Acoustics tests

The advantages and disadvantages of this technique can be summarized as follow.

Advantages:

1) The technique is not destructive.
2) The technique is quite accurate
3) The technique can be used in combination with other techniques.
4) Because it is a form of augmented visual inspection, there is no need to create a specific library of valid references.

Disadvantages

1) The test bed equipment used in this technique is quite expensive (even if relatively low cost SAM devices started to appear in the market). As a consequence, this technique is mostly used in forensics labs at the time of writing this report.
2) It can be used only for specific types of goods where the structural or mechanical differences can be used to distinguish a valid good from a counterfeit one.

4.16. Summary on the application of Authentication technologies for the fight against counterfeiting

As described in the analysis of the various techniques, one major disadvantage is related to the costs for the implementation of test beds to identify valid goods from counterfeit ones. The equipment can be rather expensive for some techniques (in the order of tens of thousands of euro to hundreds of thousands of dollars). Training costs must also be included.

(NOKOMIS, 2013) provides some estimates (provided in Table 1) for visual inspection, X-ray inspection and de-capsulation for check of Integrated Circuits (ICs) in comparison to functional tests of electronic components on the basis of their published specifications and programming interfaces.

Table 1 Estimates on the cost of different techniques

Type of test	
Visual Inspection	Visual and acetone tests: $0.05 / piece

	X-ray or decapsulation: $125 / piece
Minimal Functionality Tests	Simple devices: 1000 $ Complex Devices 3000 $
Full Functionality Tests	Simple devices: $2000 + $5 / piece Complex devices: $5000 + $7.5 / piece

The techniques are usually quite accurate and they are often based on the intrinsic properties of the goods rather than based on an element added to the good (like the RFID). In this way, the techniques are usually able to distinguish a counterfeit good from a valid one.

In many cases, the techniques require the creation of a reference library of valid models to distinguish the counterfeit devices from the valid devices. In many cases, this can be done directly by the manufacturer but it would require the definition of a new process, which does not exist not. An ideal implementation of this process would require the definition of a central entity, which stores the reference libraries for different types of goods. Manufacturers would be responsible for updating the reference library when a new model is place on the market. Then, law enforcers or consumers could use the library to identify counterfeit goods in the field. See also Section 13 on Recommendations.

Even with these challenges, authentication technologies can be quite effective in identifying counterfeit goods and they can complement very well other techniques like Container Tracking and generic Track and Trace technologies described in the following sections.

5. Track and trace techniques

5.1. Introduction

Track and trace techniques are based on the assignment of an identifying token to a product which is then used to track the movement of the product along the supply chain. The use of these technologies is associated to the use of a back-end database in which movement of the products along the supply-chain are recorded.

Following and recording the progressing of the product, through this identifier, in the supply chain is an important function which is then used by the final customer and the manufacturer of the product to check the origin and/or provenance of the product.

In "track and trace", the term "track" is related to the function the movement of the goods as they progress through the supply and distribution chains from manufacturers to the users. This is done by collecting information at some or all of the transaction points along the supply and distributions chains and uploading them to a database (Davison 2011). The term "trace" is used to represent the function of querying the database of previous transactions to have a view of the path of the good in the supply and distributions chains. One of the objectives of the "trace" function is to identify anomalies in the supply chain (like gaps).

Information about the origin and history of each tracked good (or the package) is either carried directly in the applied token (if it has enough memory to store the different points in the supply chain) or it is held in a database. There is a trade-off between the former and the latter cases. In the former case, the token must have a memory to record all the transactions. This increases the cost of the token but also provide the benefits to the final consumer (or even the law enforcer). In the latter case, the token can be quite cost-effective and the final consumer can always access the tracking and tracing information from the database if s/he is granted access. The access to the database is obviously important to empower the consumers in detecting counterfeit items and this aspect is discussed more in detail in section 12. Empowering the Consumer.

The Track and Trace tags, labels, codes may not be immune to copying of falsification, but its security is greatly enhanced by the inclusion of unique and apparently random serialization, or non-predictable numbering, ideally at individual item level. If the serialization was sequential, then the level of security would be very low as the sequence is predictable, whereas "random" serialization using highly secure algorithms or methods of encryption overcomes this. Individual packs may still be copied, but the system will identify duplicates or invalid serial numbers, as well as those which have been cancelled or expired, or which appear in the wrong market, or with invalid product details (incl. aggregated packaging information).

Where secure serialization is applied visibly to a pack, then it may be authenticated by customers via a telephone, internet link to the system, to ensure that the information is readily accessible and yet secure against compromise.

Empowering consumers to decode and verify serialized unique identifiers with mobile devices, such as smartphones, increases the likelihood of detecting non-compliant products, both counterfeit and diverted. Consumer-level verification with the use of modern-day tools also increases the awareness of the issue of illicit trade and is already used in many industries. In addition, data generated as a result of code verification could be used by the authorities to determine areas where illicit products are sold, including the possibility of identifying non-compliant supply chain operators.

There are many popular technologies, which can be used for track and tracing. In this section, we will describe the main techniques. Note that tracking and tracing information can be inserted in overt and covert elements described in section 4.7. Visual Identifiers inserted in the good. This is significant trend in recent years and it is due to the increase level of sophistication of overt/covert technologies.

The following techniques are identified, which are described more in detail in the following sections:

1. Numeric Identifier and Bar Code. This is just a numeric identifier, which can be printed on the good or the package containing the good.
2. QR Code. In a similar, way, this is a QR code, which can be printed on the good or the package containing the good.
3. RFID. This is a Radio Frequency Identifier, which must be applied to the good or the package container the good.
4. Fingerprint technology
5. Other overt technologies. This category includes other technologies, which can be embedded or applied on the good or the package. For example: an hologram.
6. Other covert technologies. This category includes other technologies, which can only be detected using special equipment. The covert element can be embedded or applied on the good or the package (e.g., a security thread)

The desirable features are similar to other counterfeiting technologies: the cost of the element itself, the organizational and technical costs to implement the infrastructure, the robustness against clonability and the effectiveness and simplicity of the detection.

An important aspect is also how the information are collected, processed and transmitted to the remote system. The amount of data to be transmitted creates restrictions on the wireless communication technology used for this purpose.

To summarize, track and trace technologies serve a number of distinct functions:

(a) Tracking an item through the supply chain, to each point where there is the facility for data capture.

(b) Providing traceability on the history of an item (electronic pedigree), subject to limitation on number of control points.

(c) Enable authentication of the data at any time, and by implication, of the pack or unit on which it is applied.

In the following sections, we will describe each of the techniques.

Before introducing each technique an overview of mass serialization technologies is provided. The subsequent sections on Bar code, QR code and other technologies can also be used in mass serialization technologies.

5.2. Mass Serialization Technologies

5.2.1. Generation of a unique secured identifier

Unique serialized identifiers marked on every product is the solution widely implemented by some Fast-Moving Consumer Goods (FCMG) industries. This more and more common solution is in compliance with GS1 standards and accessible through GS1-compliant data carriers.

A unique non-predictable serialized identifier is irremovably printed at product manufacturing time: it is a visible element. The way the unique identifiers are generated ensures (i) integrity of the data they store (ii) interoperability with systems providing additional data, and (iii) compatibility with various data carriers, including compatibility with FMCG industry standards.

To ensure integrity, unique identifiers used by some FMCG manufactures incorporate a security element. This allows the unique identifier to serve as an element of the security feature. To ensure compatibility with various data carriers, unique identifiers should follow internationally recognized standards. To meet this criteria the unique identifiers are formatted in a GS1 format, and displayed using GS1-compliant data carriers.

More specifically, unique identifiers generated by some FMCG manufactures follow serialized GTIN (sGTIM) GS1 standards, and comprise two elements:

1. A Global Trade Item Number (GTIN) that uniquely identifies the product (all items of the same product carry the same GTIN); and

2. A serial number that uniquely identifies an item within a class of product.

5.2.2. Data carriers for serialized unique identifiers.

To be effective, data carriers for a serialized unique identifier must be highly compatible with and usable by all operators across the supply chain including the logistic service providers. Global interoperability is a critical factor for a solution to be widely-accepted.

Currently, GS1 is the only global traceability standard accepted and used across all industries requiring logistic services.

Two types of data carriers are often used for serialized unique identifiers:

(i) human readable, and

(ii) machine readable.

The human readable unique identifier is applied in alpha-numeric format, and can be read by naked-eyes enabling verification by anyone without having to use any reading equipment/device.

The machine readable data carrier of the unique identifiers enables fast reading (and aims at preventing human reading errors). It can be applied in different formats, depending on (i) manufacturing speed, and (ii) limited printing space on the different packaging elements.

At high manufacturing speeds, it is important to use data carriers that can be applied to unit packets without sacrificing readability.

5.2.3. Serialized unique identifier - reading and aggregation.

The manufacturer should place the serialized unique identifiers where they can be read and aggregated into a higher packaging unit.

Reading all the codes applied on products contained in a higher packaging unit is essential for aggregation purposes, creating the so-called parent-child relationship. This ensures that each lower packaging unit (child) is linked with a unique higher packaging unit (parent). Aggregation at manufacturing time enables to track the items without

having to unpack, track individually all unit packs and repack every time these are distributed in higher packaging levels (e.g. group consumer packaging unit, and in cargo packaging units/shipping cases).

5.3. One dimension-Bar Code

This was the first technique to serialize products and use this information to track and trace the good in a supply or a distribution chain. The first implementation was the Universal Product Code (UPC) has been a dominant barcode standard in North America since it was established in the 1970s.

The UPC has evolved in various versions: UPC-A, UPC-E and so on.

At international level, the Global Trade Item Number, GTIN, is an identification number that may be encoded in UPC-A, UPC-E, EAN-8 & EAN-13 barcodes as well as other barcodes in the GS1 System.

Numeric Identifiers based on bar codes have been extensively used for many years around the world, and they remain the most used track and trace/identification technique.

Because there is an extensive literature on this technique, we refer the reader to related references. For example for GTIN, see (GS1 2015).

A Traceability Expert Group consulted by DG SANCO on product traceability has recommended in their final report (SANCO 2013) that "Key Recommendation 1 Economic operators should label their consumer products at least with a product identification code and contact details of the responsible economic operator".

5.4. QR code and other two dimensional bar codes

The QR (Quick Response) Code is a two-dimensional (2-D) barcode.

In comparison to one-dimension bar codes, the QR code are able to store more information in the same space. QR codes are designed to be read and understood (decoded) by computers, using machine-vision systems consisting of optical laser scanners or cameras and barcode -interpreting software.

Unlike 1-D bar codes, the QR Code is a 2-D matrix code that conveys information not by the size and position of bars and spaces in a single (horizontal) dimension, but by the arrangement of its of its dark and light elements, called "modules.

The QR code have a number of advantages in comparison to one-dimension bar code. The main advantage is the high-capacity data storage as a QR code can store hundreds of time more data than an one-dimension bar code. The QR code is also robust against curved surfaces or errors due to marks or spots.

QR codes are extensively used for the identification, tracking and tracing of items in the supply and distribution chain.

5.5. Physical Fingerprint Technology

Fingerprint technology is an emerging authentication solution that is being used in various domains: in 2011, the Royal Canadian Mint began using digital fingerprint technology to securely authenticate Canadian Dollar coins[2]; this technology is also used now for FMCG.

[2] www.amisdeleuro.org/upload/1340734488.pptx

Physical fingerprints use the specific characteristics of the base material of the packaging. For instance, paper, cardboard, metal and plastic are made up of tiny fibers in random orientations, which is naturally unique in its structure. According to this, every packet has its own microscopic structure, its own fingerprint, which cannot be rebuilt and cannot be removed. For a secure authentication, it is key to use this technology directly on the base material of the smallest packaging available to consumers; fingerprints of labels, stickers or banderoles will verify the attached strip but not the packaging onto which these are applied.

For greater security, it is possible to combine a printed unique identifier as the visible element and physical fingerprint of a pack as the invisible element of a security feature. On a mass production line, each packet can be scanned and its unique fingerprint can be recorded and linked to the specific unique identifier of this packet. For checking, whether a packet is genuine or not, the system compares the physical fingerprint of the packaging base material with the digital fingerprint embedded in (or retrieved from) the unique identifier present on the pack.

5.6. Other overt technologies

This section identifies other overt technologies already described in sections 4.7.2. Overt technologies which can also contain tracking information. In other words, the overt element has a serialization and identification information which, in addition to authentication, can also be used for tracking.

There are many examples already available in the market of overt technologies used for the purpose.

One example based on specific type of seal is described in (ATT 2015). The special seal is a highly secure and unique code, enabling authentication, identification and serialization of a product or of a component. The code can be applied as an overt feature (but it can also be used in covert mode), and acts as a digital data container, carrying encrypted information on a surface ranging from a few microns to a few square millimeters.

The seal may be applied on secondary and/or primary packaging or on the pharmaceutical product itself, using standard print techniques, including offset, heliography, flexography, inkjet and laser. The code can be then read on assembly lines or in the field with smart phones, thus granting protection to brand owners and consumers alike thus enabling the empowering the consumers concept as well.

5.7. Other covert technologies

This section identifies other overt technologies already described in section 4.7. Visual Identifiers inserted in the good , which can also contain tracking information.

As for the overt technologies, various products appeared recently in the market, which embed track&trace information (numbering) in the covert element.

One product based on holograms is (Rako 2015), where holograms with tamper-proof laser engraved track & trace numbering (based on laser codings) are applied to the good or the package. The laser codings are saved in central database, so that they can be retrieved and compared using a special reader.

Auhentication solutions based on a chaosmetric concept have been developed and described in ProofTag (2015). Chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions. Small differences of these initial conditions yield widely divergent outcomes for such dynamical systems, rendering long-term prediction impossible. Once stabilized, the result of certain chaotic systems can be observed and measured. The measurement of each element gives a unique result different from all other samples, which can be used to uniquely identify a good in the supply chain.

In other words, the concept is similar to biometrics that refers to the identification of humans by their characteristics or traits. Chaosmetric relies on the recording of physically unclonable features to create a serialized authentication element. The information used to generate the Chaosmetric tag is used to uniquely identify the item, so that it can traced and tracked using a smartphone.

5.8. Radio Frequency Identifier

5.8.1. Description

An RFID tag is basically a device composed of a small chip connected to a coil (see Figure 7). The chip is essentially a state machine with a memory, providing limited storage and computation capabilities. For the communication with such devices, a RFID tag reader has to be used. The reader emits a radio frequency (RF) field that by induction through the coil powers the chip. At the same time the reader properly modulates the field to code commands sent to the chip, which in turn replies to the reader modulating the same field, so establishing a bi-directional communication.

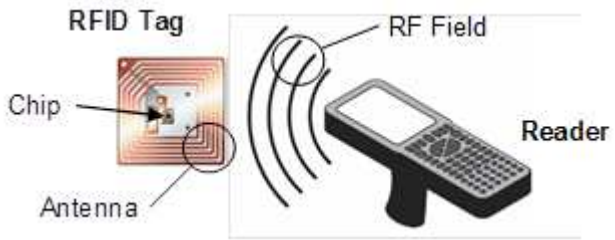

Figure 7 Radio Frequency Id

The typical purpose of an RFID tag is to memorize data and release them when queried by a reader; usually, at least a unique identifier (ID) is stored in the chip. According to this peculiarity, one of their main applications is represented by item labelling.

RFID tags can be stuck on or embedded into items to track their position, reading the tags at different places, and to easily get information about them storing specific item-data in each applied tag. The information gathered from a tag can also be put in relation with additional item data stored in a back-end system.

Figure 8 describes the generic architecture a system for the tracking of goods. A tag is attached to the good, which moves in the supply chain. Personnel involved in the supply chain process, can use a portable leader to inspect a RFID tab. In alternative a fixed reader placed in strategic points in the supply chain (e.g., intermodal exchanges) connected to the control centres can also be used.

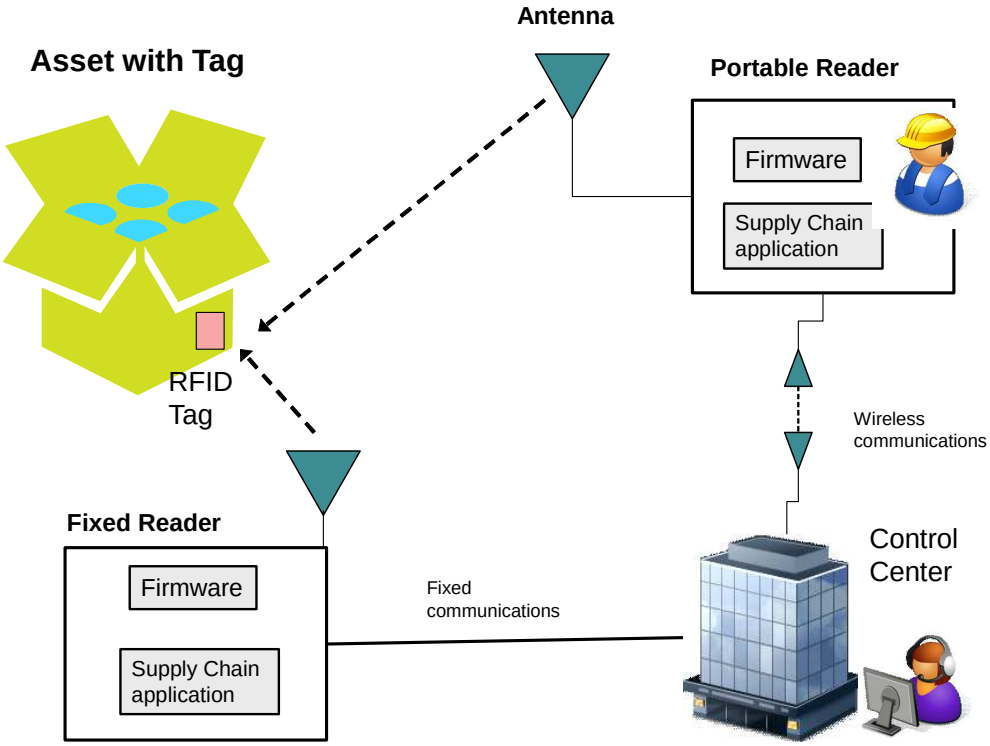

Figure 8 Generic architecture for tracking of goods through RFID

Some simple anti-counterfeit solutions could be derived by the regular usage of RFID tags and the relative back-end systems. For instance, if tag transactions are recorded and a tag is cloned, at a certain moment two or more ID entries could appear in the back-end system, so highlighting the presence of a possible counterfeited item. Alternatively, a transaction counter synchronized with the back-end system could be adopted on each tag and discrepancies between the current tag counter and the current back-end system counter for the specific tag's ID would highlight the presence of a clone. The ID of a compromised tag could be also blacklisted. Differently from cloning, whether a fake tag is applied to a good, the relative ID could not be registered in the back-end system, so triggering an alarm. For such solutions a unified database/back-end system able to track item transactions/movements across organizations (e.g., product manufactures and reseller) would be necessary, but it seems not-plausible at the moment as many organizations tend to use custom solutions and scarcely cooperate together. This basically impairs the adoption of the above-mentioned solutions nowadays. In addition, a connection with the back-end system would be always required. Probably, more practical off-line solutions should be preferred in lieu of on-line ones.

EPCglobal® is leading the development of industry-driven standards for the Electronic Product Code™ (EPC) to support the use of Radio Frequency Identification (RFID) in today's fast-moving, information rich, trading networks. The EPC is a unique number that is used to identify a specific item in the supply chain. The EPC is stored on a RFID tag, which combines a silicon chip and an antenna. Once the EPC is retrieved from the tag, it can be associated with the data held in a secured database, such as where an item originated or the date of its production. Much like a global trade item number (GTIN) on the barcode or vehicle identification number (VIN), the EPC is the key that contains the information used within the EPCglobal Network. An EPC tag does not carry personally identifiable information. Several major retailers and product manufacturers

are testing EPC technology as a way to improve supply chain management. Similar to the VIN on a car, an EPC is a way to uniquely identify a pallet, case, or individual product. A major standardization initiative by GS1 is Electronic Product Code Information Services (EPCIS) EPCGlobal (EPCIS (2014)), which is an EPCglobal standard for sharing EPC related information between trading partners. EPCIS provides important capabilities to improve efficiency, security, and visibility in the global supply chain, and complements lower level EPCglobal tag, reader, and middleware standards. EPCGlobal has highlighted the need for standards to combat counterfeiting in a recent white paper (EPCGlobal (2012)).

5.9. Other track and trace technologies

Other tracking technologies can be based on a combination of other technologies, which can be even more sophisticated than RFID. Here we briefly describe some of them, but the technology landscape can change in time:

1. Products similar to RFID but with a simpler design. Like radio frequency tags based on different standards and design than RFID.
2. Use of Global Navigation Satellite Systems (GNSS) receiver to track the position of the goods with greater precision.

In the first category, we have products like the one described in SECRF (2015) (Lime Tag), which are based on a secure Near Field Communication (NFC) solution that includes authentication and encryption protocols. These type of products can be used in many applications like the tracking and tracking of bottles of wines.

In the second category, we have products, which embeds a GNSS receiver to record the positions of the good at certain time. While this type of devices have been mostly used for tracking of container, recent development and the drop in prices can support their usage for track and trace of small packages.

5.10. Analysis of track and trace based techniques for the fight against counterfeiting

As described in the previous sections, different techniques can be used to support track and trace, even if each technique has its advantage and disadvantages. A recent report from NIST (NIST 2014) summarizes the main difference and advantages/disadvantages of the two approaches.

The advantage of bar code/QR code and other overt/covert techniques in comparison to the RFID is the cost of the token itself even if the cost of RFID has decreased considerably in recent times. As described in (NIST 2014), barcode labels cost less than 2 cents per label while RFID tags are at least three times more expensive per tag. The precise cost of RFID tags varies depending on the underlying RFID technology, but typically, active RFID tags are priced between $20 and $70, whereas passive RFID tags are between 7 and 20 cents.

The disadvantages of bar code and QR code in comparison to RFID are that (Davison 2011) that a direct line of sight is requested between the reader and the code. In addition, the presence of visible light is needed with nothing obstructing the light path between them. Instead, RFID tags can be read at a distance and UHF and BAP RFID can be read at even a greater distance and can be scanned much faster (NIST 2015). RFID tags can also be read and written in large numbers. This is an important advantage to be taken in consideration. While, bar code are considerable cheaper, the bulk interaction with tagged items reduce the time in the supply chain and therefore reduce the costs. A study on the Bloomingdale chain (O'Connor 2009) has shown that with barcodes, staff was able to read 209 items/hour, while with RFID, staff was able to read 4,767 items/hour.

Another advantage of RFID technologies is the possibility to embed intelligence and algorithms, which cannot be done in bar codes: intelligent chips can be programmed to accumulate data for local storage, periodically wake up to perform functions and protect their data or onboard functions with encryption or passwords. Note, that the RFID tags, which can perform this wide range of functions have relatively high costs.

Regarding the application of the RFID specific technology, the general concepts of the application of Track and trace based on RFID technology against Counterfeiting are presented in (Li (2013)) where the typical manufacturer, distributor, and retailer elements are identified. At the manufacturer, an RFID tag is attached to the finished product. As described before, the tag may include information like producer's identity, product code, production date, container id and so on.

After the product arrives at the distribution centre, the information saved on the attached RFID tag is read and transmitted to the manufacturer's data server to support the cross-correlation of information and therefore the authentication. This operation can be repeated at different stages and nodes (e.g., warehouse) in the distribution network to ensure that no counterfeited products are inserted in the distribution chain. When the product finally reaches the retailer the authentication is carried out in a similar way to the other points in the distribution chain. The retailer can keep the RFID for internal tracking until the product reaches the customer.

Various references provide a costs analysis of the deployment of RFID infrastructures.

First of all, the costs of implementing a track and trace infrastructure based on RFID technology should divided for the different components of the infrastructure. (Banks et al. (2007)) provides the following structure in Figure 9.

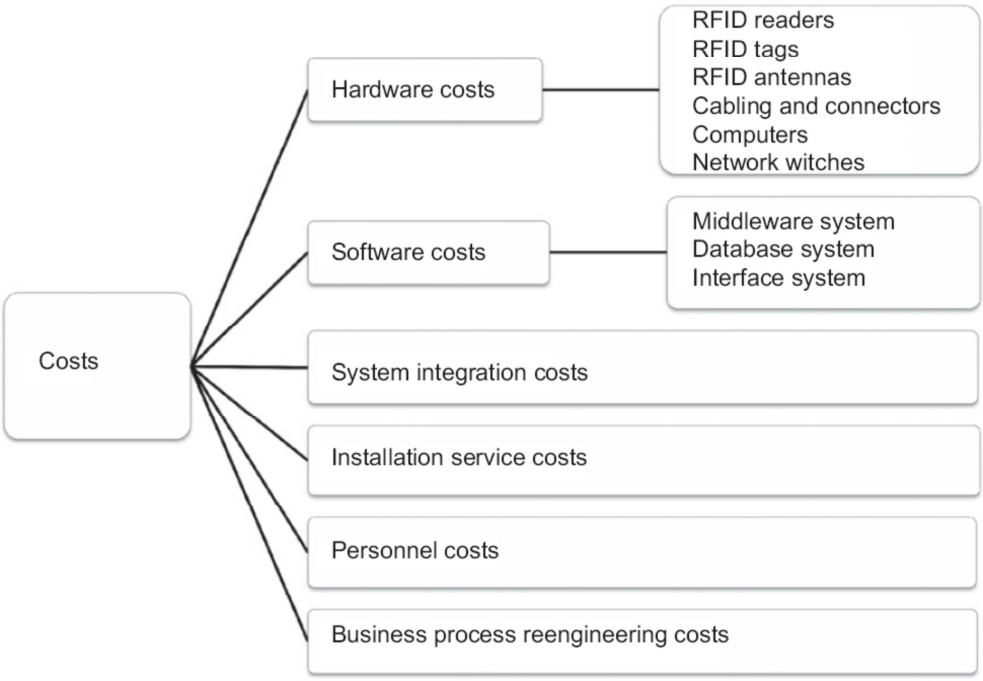

Figure 9 RFID implementation cost tree from (Banks et al., (2007)).

An analysis of the associated costs in RFID implementation was provided in (Smart et al (2010)), which examined the costs associated with the adoption of RFID in the automotive industry. The study found that, with the exception of the costs of tags, direct implementation costs were not significant for early adopters (Smart et al., (2010)).

A simulation of the costs associated to the introduction of the RFID in a supply chain is also provided in (Sarac et al, (2008)). A tool has been created by the authors, which is used to simulate the costs in different scenarios

Track and Trace can be an effective way to mitigate counterfeiting in relation to counterfeited goods, because such counterfeit good will not carry a valid RFID installed by the manufacture and the mismatch between the stored value of the RFID in the central server and the check at any place of the supply chain (including the final customer) can expose the counterfeit products. A similar consideration can also be applied to overt and covert techniques described in the previous sections.

In fact, track and trace based on RFID has been used to mitigate counterfeiting by various companies. Examples include GUCCI as described in (Li (2013)) or the SecureTrace as described in (Pharma IQ. (2011)) has been combating counterfeiting in the United Kingdom for some time.

Even if it is widely deployed, track and trace against counterfeiting have the following issues:

1. The cost of implementing and maintaining a complete track and trace supply chain can be quite high, even if the individual RFID itself has a very low cost. On the other side of the coin, the implementation of track and trace in a supply chain can provide additional benefits not strictly related to fight against counterfeiting. This was highlighted by a recent study by (De Souza et al. (2011)), which evaluated the Return on Investment (ROI) of the implementation of track and trace for a company in Singapore.

2. RFID can be easily cloned. One solution against clonability would be to implement cryptographic algorithms on the challenge/response of the RFID (i.e. Secure RFID). Even if a new generation of secure RFID has been developed in recent years (one example is reported in (Liao, Y. P., & Hsiao, C. M. (2014))), the cost of secure RFID is higher than basic RFID. The supply chain must also be implemented in a more complex and costly way for the authentication elements based on the cryptographic algorithms.

3. RFID can generate a privacy threat if the RFID is not deactivated after the point of sale (see also section 12.3. Privacy). If the RFID is not secure (protected by encryption), the content can be read at distance by any person equipped with an RFID reader. This privacy threat was highlighted in the Benetton case, where Benetton was forced to abandon the plans for the adoption of RFID (see Simson et al (2005)). Various deactivation techniques exist (one is described in Chen et al. (2011)) but they can also add costs to the implementation of track and trace. In fact, the privacy threats in RFID can have an "ethical" cost as underlined in (Bhattacharya et al., (2007)) or in the automotive industry (Smart et al., (2010)).

4. To be really effective, track and trace based on supply chain should support a smoothness integration and correlation of data among all the stakeholders involved in the supply chain including the customer (see (Pharma IQ. (2011))). The integration of the various data server add complexity to the overall deployment of track and trace solutions because ICT systems could be different in the various parts of the supply chain.

5. Even if traceability has a high value in helping to pinpoint counterfeit items, it does not fully answer to the problem of product security. As described in (Davison 2011), it is also important to answer the question "Is this product genuine or a fake ?". The token can be duplicated or modified (even if some techniques presented later have solutions to prevent clonability) or even the database can be hacked. While, some track and trace technologies are able to insert the token in the good itself, so that the token cannot be removed without destroying or damaging the item in a visible way, many categories of products (e.g., electronic components) can only use an applied token. For these categories, only authentication techniques can provide the answer of the proper identification of the product.

Even with issues, track and trace is one of the most popular approach against counterfeiting related to Counterfeiting as described in (Michael and McCathie, (2005)).

6. Container tracking, packaging and sealing

6.1. Container tracking

6.1.1. Introduction

The tracking of the container shipping around the world is another effective way to mitigate counterfeiting. As described in the UNODC report (UNODOC 2014), a large percentage of the containers stopped by authorities have involved counterfeit goods.

The United Nations Office on Drugs and Crime and the World Customs Organization (WCO) have elaborated the UNODC-WCO Container Control Programme (CCP) to mitigate counterfeiting risks with to minimize the exploitation of maritime containers for the illicit trafficking of drugs, and other transnational organized crime activities

The main concept is to track a container from the port of origin to the port of destination by collecting the information on the routes of the freight containers.

An example of a system for the tracking of the containers developed in the DG JRC is described in the following section. This case study shows what is the potential of container tracking in the fight against counterfeiting.

6.1.2. ConTraffic project

ConTraffic is a project started more than 10 years ago by JRC in collaboration with OLAF and DG TAXUD which aims at supporting customs authorities dealing with the control of containerised cargo. The goal of the project is to develop novel methods and IT tools that assist authorities in their risk assessment activities.

About 90% of the international traded non-bulk cargo is transported by maritime means in intermodal freight containers, whereas less that 2% is physically inspected by customs authorities. Authorities use mainly risks analysis methods to identify which containers to control in order to fight criminal and illicit activities, such as smuggling of arms, drugs, cigarettes, counterfeited goods or avoidance of customs duties and anti-dumping quotas. In their risk assessment, customs officers analyse various information in order to develop risk profiles that can help them to ultimately identify suspicious consignment.

Normally risk analysis and controls done by customs are based either on information about the entities involved (shipper, consignee, customs broker, agent, etc…) or characteristics of the goods (tariff classification, value, weight, etc…) or other information provided by the entities involved (for example the origin country in the SAD declaration).

The origin, destination, transhipment locations and the complete route of the cargo transportation is considered an important factor in the risk analysis for the profiling & targeting of high-risk cargo containers.

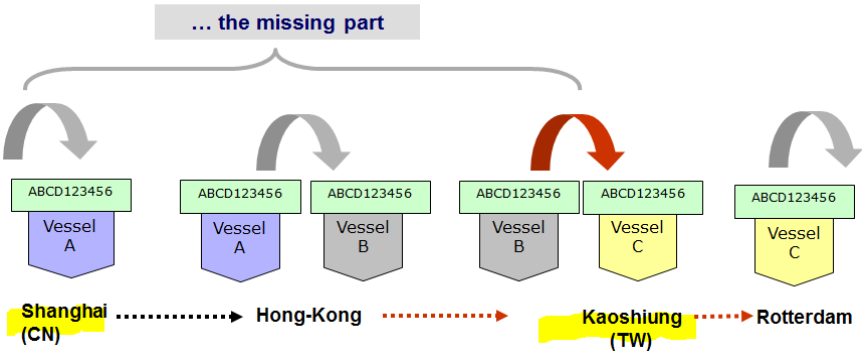

Figure 10 The container flow in ConTraffic

In most of the cases, authorities have very limited or incomplete information about the actual global routes of the containerized cargo and they do not use in a systematic way the data that describe the itinerary, status and movement of shipping containers. On the other hand, ocean carriers, which transport the cargo containers, collect, store and own Container Status Messages (CSM). These records describe the global movement and status of the containers and provide an independent source of information which complements the information available to Customs and other authorities.

The key idea of ConTraffic is that CSM data can efficiently be used to reconstruct the route of containers and can systematically be used to perform route-based risk analysis and to support on-going investigations.

6.1.2.1. Container Status Messages

The ocean carrier companies, which transport millions of shipping containers between thousands of locations in the world, need to keep track of their fleet of containers and the progress of their transportation. Such companies interact with thousands of logistic operators around the globe that handle the various stages of the transportation.

A key component in the success of the intermodal shipping container industry is the early adoption of EDI technology. This technology, through the various widely accepted standards, allowed the involved companies to electronically exchange information regarding the logistic operations. A key type of message exchanged between parties is the so-called *Container Status Message*. This type of EDI message is used to report the status or operation performed on a shipping container. Ocean carriers depend on the collection and processing of those messages, as it is the only way they can keep track of their fleet of containers and monitor the progress of millions of shipments. The Container Status Messages (CSMs) are generated by various parties involved in the handling of containers but most of them are generated by container terminals and depots. Ocean carriers collect the CSMs using the EDI technology. Each carrier company is then transforming, processing and storing these messages in order to be able to use them for their day-to-day business. Finally, most of the carriers provides CSMs information on their publicly accessible Track and Trace web site to inform their customers about the status of consignments.

The CSMs may contain a big variety of data elements, depending also on the standards used to implement them. However, for the purpose of using them for route-based risk analysis the required data elements are just the following: Container identifier, Event description, Location identification, Data and time of the event, vessel, Load status (empty/full), Name of the carrier company.

Experience in ConTraffic shows that these data elements are enough to understand the movement of the containers and the routes followed during their transportation. CSM records can be very valuable for route-based profiling of shipping containers. The events described in these CSMs indicate the locations and dates when the various operations

took place. They indicate how long a container remained in a particular location and how long it took to be transported from one location to the next. They also indicate which vessels were involved in the transportation. With this information, an algorithm can answer questions like “has the container stopped in a port X for more than Y days”.

6.1.2.2. ConTraffic IT system

ConTraffic built an experimental online system that allows authorities not only to have access to container itinerary data but also to extract useful information from it and use this information for risk analysis. Currently there are about 800 registered users, mostly from MS Customs Authorities accessing these services on a 24/7 basis.

The back end of the system is composed by three main processes: Gathering of CSMs data, Processing and storage of data, and Data mining.

The gathering service runs continuously and is used to collect CSM data from the carriers' track and trace web sites. The JRC ConTraffic system is not an operational system and, as such, is capable of tracking a rather limited amount of containers worldwide (30-40% or more for imported containers). The database contains at present more than 2.3 billion Container Status Messages (CSM) covering events that took place over the last 12 years. In June 2015 it contained data for about 9 million distinct active containers.

Once CSMs for a container are retrieved by the gathering process, the records are processed and stored in the ConTraffic database. The pre-processing includes data cleaning and normalisation. As part of the cleaning process there is the normalisation of the locations (from free text to UN location code) and event descriptions.

The last process extracts from the collected CSMs, which are a raw list of simple events, the collection of information useful to calculate risk indicators and perform advanced query. In ConTraffic this collection of information is called Container Trip Information (CTI). Each CTI summarizes the available information about the transportation of goods from an origin location to a destination location in a particular container. The aim is that the CTI indicates where and when the goods have been stuffed in the container, what was the maritime route of transport (first port of loading, transhipments, port of final discharge) and where was the final destination of the goods (the place where the container was stripped to become empty).

The front end of ConTraffic is a web site which provides access to a number of online services:

- "Track and Trace" is the main and most used on-line service of ConTraffic. It allows the user to get information of Container Status Messages (CSM) of one or more containers in a specified time period (historical movements in the ConTraffic DB) or in real time from the carrier web site.

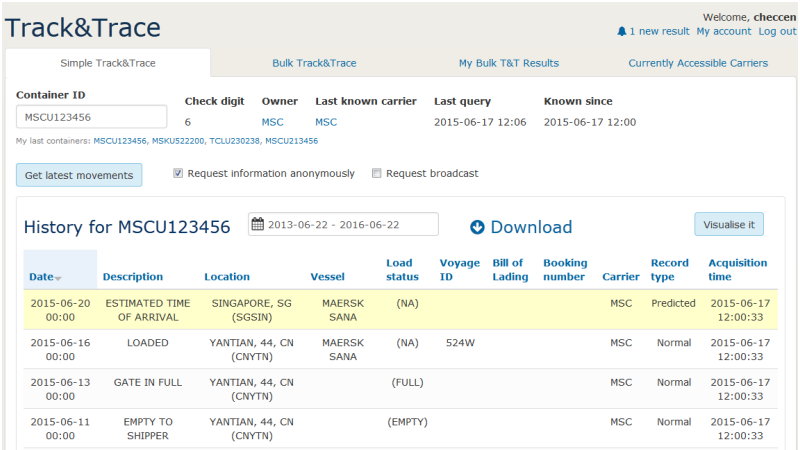

Figure 11 Tracking screen in ConTraffic

- Container Surveillance is an on-line service that tracks in near real-time the movements of specific containers entered in the system by the users. The application notifies (by email) the users of any detected new movements of the containers they have entered for tracking.

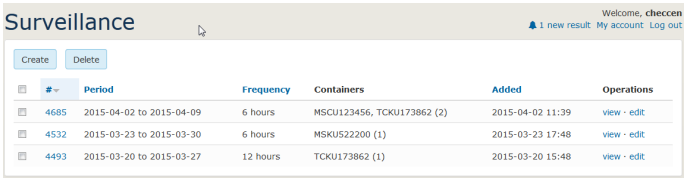

Figure 12 Tracking of specific containers in almost real time.

- Port2Port is an application that shows the results of pre-computed statistical analysis on the logistic routes followed by carriers to transport containers between particular departure and destination ports. The graphs for the pre-calculated pair or departure-destination ports (of a particular carrier) show which logistic routes have been used by the carrier over a period of time and with what frequency, identifying any possible outlier (abnormal logistic route).

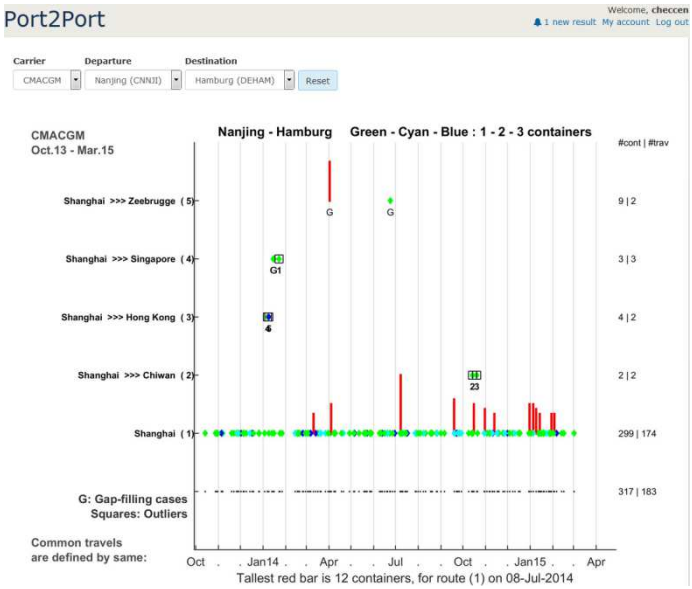

Figure 13 Pre-computed statistical analysis on the logistic routes followed by carriers to transport containers

- Visual Analytics is an application that allows the user to interactively explore all the data in the ConTraffic database. Visual Analytics allows searching and visualising Container Status Messages (CSM) but also other information derived from the initial CSM data like the CTI. A Visual Analytics session is normally composed by a first selection of the data to be displayed, followed by the visualisation of selected data and finally by the interaction with results for further refinement of the selection criteria leading to new visualisations.

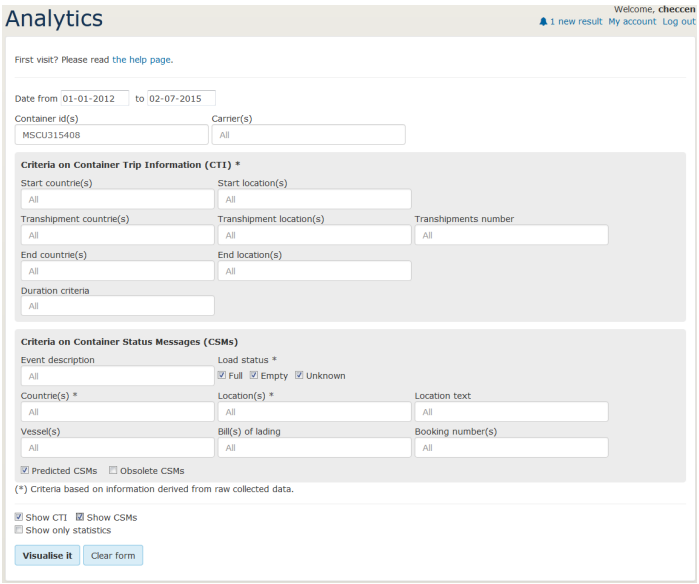

Figure 14 Visual analytics in ConTraffic

Once the selection criteria have been set, the selected information is visualized as a geographical map, timelines and text tables. The map shows the spatial distribution of the selected information. Symbols are represented at some locations where some information has been found. These symbols are usually pie charts representing the

information distribution by type. The symbol's size depends on the amount of information. Connecting lines represent estimated maritime routes related to the selected information.

Figure 15 Information selection in ConTraffic

The timeline shows the distribution of the selected information across time. For each container, several timelines are shown, depending on the selected information.

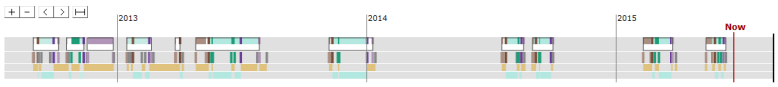

Figure 16 TimeLine of a container

6.1.2.3. ConTraffic Pilot Projects

A number of pilot projects have been initiated based on the ConTraffic IT infrastructure and data.

One of this is the ConTraffic SAD Analysis project. JRC, in collaboration with OLAF and 12 MS Customs, has been developing an experimental system to provide for automatic cross-checking of the origin declared by importers in the SAD datasets, supporting MS Customs Authorities in the detection of potentially fraudulent declarations and validation of investigative results.

The SAD Analysis system identifies the cases for which the declared country of origin is different from (or not compatible with) the country estimated by using the Container Status Messages. The detected fraud is the one of mis-declaration of origin (quota, preferential duties, anti-dumping) and not the ones of smuggling, misclassification or under-valuation. The results of this pilot project have been used by OLAF to propose the amendment of (EC) 515/97.

Another project is C-ENS. It aims to study the methods that combine container itinerary information with Entry Summary Declarations (ENS, advanced cargo information) for the real time targeting of high risk containers posing security and safety threats. The project is implemented with the participation of 7 customs authorities and under the guidance of DG TAXUD.

6.1.2.4. Analysis of ConTraffic for the fight against counterfeiting

In the context of the fight against counterfeiting, ConTraffic can support evidence in ongoing investigations by providing an additional source of information. For good results in detecting counterfeiting, it needs to be used together with other information such as bills-of-lading or customs declarations; ConTraffic does not possess data on the products inside containers but only on their routes.

ConTraffic cannot track individual shipments and can be used only when the goods are transported in containers by ocean carriers and the identifiers of the containers carrying the goods are known. If this is the case, an investigator can easily explore the ConTraffic database and get information like the route followed by the container, the location where it was stuffed with goods, the transhipment ports, the handling time for each transport phase, the vessels involved, etc…

6.1.3. Standards and standardization activities for Container Tracking

Beyond the ConTraffic project described in the previous sections, there are numerous standardization activities and standards related to container tracking, which are identified here:

1. Standard: ASTM D5728-00 Standard Practices for Securement of Cargo in Intermodal and Unimodal Surface Transport. These practices are intended to serve as a guide to shippers, carriers, and consignees for load planning, loading, blocking, and bracing of intermodal and unimodal cargo in surface transport. The practices are referenced to a bibliography of information concerning the above. Hazardous materials, bulk cargo, non-containerized break bulk in ocean carriage, and transport of cargo by air are not included in these practices at this time. The practices are intended to form a framework for the safe and effective loading and unloading of cargo in intermodal and unimodal surface transport. This standard does not purport to address all of the safety concerns.
2. Standardization Activity: ISO TC204 Intelligent Transport Systems: security intermodal freight, transport of dangerous goods, real time tracking of transported goods with RFID, on board computing and mobile communication with vehicles. Transport telematics on the worldwide level is being solved mainly in the frame of the technical committee ISO TC 204 Intelligent Transport Systems. Some of the working groups of the ISO overlap in their activities with the working groups of CEN, as shown below. Other working groups do not have a European equivalent. Relevant Working Groups for container transportation are:
    - WG1 - Architecture
    - WG3 - TICS database technology
    - WG4 - Automatic vehicle and equipment identification
    - WG7 - General fleet management and commercial/freight
    - WG9 - Integrated transport information, management and control systems
    - WG11 - Route guidance and navigation systems
3. Standardization Activity**:** TC 104 Containers. Standardization of freight containers, having an external volume of one cubic meter (35.3 cubic feet) and greater, as regards terminology, classification, dimensions, specifications, handling, test methods and marking. The TC will provide current standards that continue to define intermodal freight containers, related equipment and technology applicable to the intermodal, containerized movement of freight. Specific areas of expertise codified or being codified in TC 104's series of

standards includes design and testing of all types of intermodal freight containers, terminology, equipment to secure freight containers to vessels and other conveyances, container handling equipment, electronic tagging and identification of containers and their contents, electronic and mechanical container seals, power line transmission of data relating to electrically powered containers such as refrigerated containers, electronic data interchange message formats, container markings and container security from a design perspective.

4. Standardization Activity**:** ISO TC 8 Maritime. This is the general committee for ships and marine technology. In particular, TC 8/SC 11 is the subcomitte for intermodal, inland navigation and short sea shipping.
5. Standard**:** ISO 9897:1997 Freight containers – Container equipment data exchange (CEDEX) – General communication codes
6. Standard**:** ISO 17363:2007 Supply chain applications of RFID – Freight containers
7. Standard: ISO 17363:2007 defines the usage of read/write radio-frequency identification technology (RFID) cargo shipment-specific tags on freight containers for supply chain management purposes (shipment tags). It defines the air-interface communications, a common set of required data structures, and a commonly organized set of optional data requirements (through common syntax and semantics).

It contains recommendations about a containerized cargo supply chain RFID system, based on shipment tags; specific recommendations about mandatory non-reprogrammable information on the shipment tag; and specific recommendations about optional, re-programmable information on the shipment tag.

8. Standard: ISO/TS 10891:2009 Freight containers – Radio frequency identification (RFID) – Licence plate tag.

ISO/TS 10891:2009 establishes:

- a set of requirements for container tags, which allow the transfer of information from a container to automatic processing systems by electronic means;
- data coding system for container identification and permanent related information which resides within a container tag;
- data coding system for the electronic transfer of both container identification and permanent related information from container tags to automatic data processing systems;
- the description of data to be included in container tags for transmission to automatic data processing systems;
- performance criteria necessary to ensure consistent and reliable operation of container tags within the international transportation community;
- the physical location of container tags on containers;
- features to inhibit malicious or unintentional alteration and/or deletion of the information content of container tags when installed on a freight container.

It is intended to be applicable to freight containers as defined in ISO 668 as well as to other containers not defined in ISO 668 and container ancillary equipment such as road and terminal chassis, generator sets and power packs.

9. Standard: An important element of the Container Tracking is the exchange of messages among control centers for container tracking. For this function, the following standards are used:

- ISO 17687: Data dictionary and message sets for electronic identification and monitoring of hazardous materials/dangerous goods transportation
- ISO 24533: Electronic information exchange to facilitate the movement of freight and its intermodal transfer
- ISO 26683: Freight land conveyance content identification and communication.
- ISO 15638: TARV - Telematics Applications for Regulated Commercial Vehicles
- ISO 17262: AVI / AEI Automatic Vehicle and Equipment Identification – Intermodal goods transport numbering and data structures.

6.2. Container seals

6.2.1. Description of the technology

Container seals technology focuses on maintaining the physical integrity of the closed container doors by means of mechanical seals. Every attempt to trespass on the container should leave behind evidence on the seal.

Tamper-indicating seals have been in use for well over 7,000 years and are still widely used today for sealing of freight containers.

We have to distinguish between a seal and lock. Unlike a lock, a seal is not intended to delay or discourage unauthorized entry. Instead, a seal is meant to leave behind unambiguous, non-erasable evidence of unauthorized access.

There are devices, also called "barrier" seals, which are devices that are part lock and part seal. Barrier seals have their uses, but the downside is that they may not be optimal lock nor the optimal seal for freight containers.

Container seals are typically affixed to the door end of the freight container. They are used to secure the freight container in a manner that provides an indication of tampering with the seal if an attempt is made to open the container doors. Different seal types provide evidence of tampering in different ways, from scratches or nicks on the body of the seal to a deformation of the locking mechanism (from (Bohlman (2005)).

A container seals based on RFID technology is shown in Figure 17.

A list of standards for seals is provided here:

1. ISO/PAS 17712:2006 Freight containers – Mechanical seals

ISO/PAS 17712:2006 establishes uniform procedures for the classification, acceptance and withdrawal of acceptance of mechanical freight container seals. It provides a single source of information on mechanical seals which are acceptable for securing freight containers in international commerce.

2. ISO/PAS 17712:2003

ISO/PAS 17712:2003 establishes uniform procedures for the classification, acceptance, and withdrawal of acceptance of mechanical freight container seals. It provides a single source of information on mechanical seals which are acceptable for securing freight containers in international commerce.

ISO/PAS 17712:2003 is not applicable to special-purpose seals, such as fibre-optic and sophisticated electronic seals.

3. ISO 18185-2:2007 Freight containers – Electronic seals

ISO 18185-2:2007 specifies a freight container seal identification system, with an associated system for verifying the accuracy of use, having:

- a seal status identification system,
- a battery status indicator;
- a unique seal identifier including the identification of the manufacturer;
- a seal (tag) type.

Figure 17 An example of container seal based on RFID technology from (Stringa (2010b))

6.3. Packaging

Packaging is another technique, which can deter counterfeiting (Ling, 2013). Authentic logos, seals, and security printing can be included in packages to help indicate that the content and the package are genuine. The analysis on packaging can be similar to what already described in section 6.1. Container tracking for the containers obviously on a smaller scale. Packaging can be broadly categorized to primary, secondary, and tertiary. Primary packaging is the material that wraps or holds the product and is in direct contact with the contents. Secondary packaging is outside the primary packaging and is used to group primary packages together. In addition to primary packaging and secondary packaging, anti-counterfeit labels, seals, barcodes, and EPCs on packages can provide additional layers of product protection. Tertiary packaging (e.g., containers) is used for bulk handling to make loading and unloading convenient.

An extensive study on anti-counterfeit packaging technologies is provided in (Dhar, 2009), which identifies a classification of technologies. Most of the technologies have been already identified in the report, but they are applied to packaging in (Dhar, 2009).

(Dhar, 2009) proposes two taxonomies. One is based on Usage Criteria and the other is based on technological solutions.

Taxonomy based on Usage Criteria

- *Overt (Visible) Features*. Such features will normally be prominently visible, and difficult or expensive to reproduce.

They include:

  - Film wrappers, which is a transparent film with a distinctive design wrapped securely around the package.
  - Shrink seals and bands. Bands or wrappers with a distinctive design are shrunk by heat or drying to seal the cap and container union.
  - Breakable caps. Such caps break when an attempt to open it is made.

- *Covert (Hidden) Features*. The purpose of a covert feature is to enable the brand owner to identify counterfeited product. The general public will not be aware of its presence nor have the means to verify it. For example, Encrypted text visible under special light embedded in the package surface or the package itself.

- *C. Forensic Markers*, which can be considered a type of covert feature but which require more sophisticated means to authenticate the package.

- *Track and Trace technologies*, which have been already extensively discussed in this report and they are described below for packaging.

Taxonomy based on technological solutions

- *Serialization.* Like the use of Bar-codes, QRCode and RFID already described in this report but applied over the package.
- *Packaging design,* where techniques includes both identification solutions and sealing technologies for packages. The identification solutions can be implemented with a specific type of paper, a substrate on the surface of the package or labels. The labels can be of different types: from holograms labels to transfer label or multi-layered labels. The sealing technologies include secure packaging tapes or tear tapes/bands or even a liner carton.

For a detailed discussion on the advantage/disadvantages of the different techniques applied to packaging, see (Dhar, 2009).

6.4. Analysis on Container tracking, packaging and seals technologies for fight against counterfeiting

As described in the previous sections, the main purpose of container tracking and seals technologies is to ensure that the goods are safely transported from the point of origin to the point of destination, they are not tampered with and no illegal or counterfeited products are introduced in the container.

The threat of using container to transport counterfeit goods is real as reported in (UNODC (2014)), which highlights that evidence gathered from the results of the joint UNODC / World Customs Organization Global Container Control Programme (CCP) on the extent of illicit trafficking of counterfeit goods by sea. Between January and November 2013, more than one-third of containers stopped for inspection by CCP teams worldwide, and subsequently seized, have involved counterfeit goods.

As described in https://www.unodc.org/ropan/en/BorderControl/container-control/ccp.html, the Global Container Control Programme can be very effective in addressing counterfeiting due to Counterfeit, but it requires inter-agency information exchange among the main government agencies (e.g., Customs office) among the world.

An advantage of container tracking and seals technologies is that they are already implemented and deployed for other reasons (e.g., safety of the goods, mitigating stealing risks) than fight against counterfeiting. As a consequence, in comparison to other approaches, the incremental costs in the fight against Counterfeit are limited and mostly related to the exchange of information among the main agencies and data centres.

Beyond tracking, packaging of the goods is a very effective technique against counterfeiting when combined with overt/cover features or track and trace techniques, which allow the tracing of the good in the supply and distribution chain. The main disadvantage of packaging is that goods inside the package can be remove from the package and substituted with another good. In this case, sealing could mitigate this risk.

7. New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things

7.1. Techniques for fight against counterfeiting in E-Commerce

7.1.1. Description of the technique

In recent time, the counterfeit market has increasingly been going online, where it can be easier to trick buyers with slick websites and photographs copied from genuine retailers. This is a significant change from the traditional means to distribute counterfeit items, which involved shipping companies and retailers, as the counterfeit items can be sold directly online. The impact on the fight against counterfeit items can be significant because counterfeit goods no longer come in through containers but they are being shipped directly to consumers. While the physical ports of entry can be similar and still under control of customs officer, the procedures for checking containers or small packages can be different. This new trend requires new tools and approaches to detect counterfeit items. Various types of products can be bought through mobile e-commerce sites including shoes, apparel, luxury, accessories and other design-oriented goods as well as medicines and electronic consumer products. While the authentication methods described in section 4 can be used to identify counterfeit goods, new approaches must be defined.

As described in the report Situation Report on Counterfeiting in the European Union (OHIM, EUROPOL 2015), the distribution of counterfeit products through e-commerce is rising.

We can identify four main e-commerce channels of distribution of counterfeit products (OHIM, EUROPOL 2015):

1. Fake website, which try to emulate the proper websites. Some websites are of such high quality and sophistication that they rival (and in some cases are even better than) those of the rights holder. The fake website uses similar names or similar appearance of the proper web site to cheat the customer (also called cyber squatting or domain squatting).

2. Web blogs or social network websites, which sells counterfeit items. The blogs or website can be independent or associated with well-known social networks. Even if blogs or social networks do not sell directly counterfeit products, people commenting on them, can suggest places where they can buy counterfeit products.

3. Proper e-commerce retailers including auction sites, which do not control properly their distribution and supply chain and sell unknowingly counterfeit products. Many cases have been reported of lawsuits against large e-commerce retailers for the sale of counterfeit products.

4. A growing area is mobile apps such as Instagram, depop.com and whatsapp. Depop is a mobile app that works like eBay but is only available on your phone. In some cases, messages are sent directly to people to suggest websites (case

1), which offer large discounts off popular brands. (Disclaimer: these companies and web sites are only cited as examples; this report does not suggest in any way that these mobile app are responsible for the distribution of counterfeit products).

One essential challenge for the fight against counterfeiting in e-commerce is that many authentication techniques are not applicable because the physical good cannot be touched or seen directly. Rather an image is provided on the web site, which can be of dubious quality or it can be just a copy of an image of the valid product but it is not related to physical good (i.e., counterfeit good) actually sold.

Different approaches are needed to address the identified cases.

7.1.2. Fake website

Regarding the problem of fake website, countermeasures are based on the analysis of the fake websites through different means: either by simple reporting of consumers, by private companies specialized in brand protection, scouting by law enforcement organizations (e.g., Interpol, EUROPOL) or by analytical tools. Examples of companies specialized in brand protection against e-commerce counterfeiting are BRANDSTRIKE (2015) and NETNAMES (2015)

A very good and successful example of fight against Fake Websites has been "Operation In Our Sites", a joint effort by Europol and US ICE to tackle websites selling counterfeit products, has led to the seizure of more than 2 600 domain names since the operation started in June 2010 (US ICE 2015) and (OHIM, EUROPOL 2015).

Another government initiative is from USSTOPFAKES (2015) from the US Government, which was launched to serve as a one-stop shop for U.S. government tools and resources on intellectual property rights (IPR). The federal agencies behind STOPfakes.gov have developed a number of resources to educate and assist businesses, particularly small and medium-sized enterprises (SMEs), as well as consumers, government officials, and the general public. One of the main focus areas for STOPfakes.gov is the identification of fake web site and general distribution of counterfeit items on the web.

The analysis of the e-commerce web sites and the content provided through the web site can be performed through:

1. Analysis of the features of the e-commerce web site itself to identify malicious activities. Examples of features could include the methods of payment (e.g., bitcoin instead of traditional credit cards), the presence of fake logos on a web site or a similar structure of brand e-commerce web site. In other words, an e-commerce website selling counterfeit products could be designed to be quite similar to a brand e-commerce website to cheat potential customers
2. An analysis of the images of the products sold online or complementary information (e.g., serial numbers).

Regarding the first approach, the analysis could be *human-based* or *machine-based*. In the first case human-based, the e-commerce web sites are identified on the basis of the reports by web users. Reports could be sent to enforcers agencies to notify a suspect "web site". Enforcers themselves could conduct this analysis using more powerful tools based on web crawling or statistical analysis. Such analysis can be done by the companies owning a brand themselves. For example, UGG Australia has a service (http://counterfeit.uggaustralia.com/), where users can detect if another web site is selling counterfeit products or not. Another successful example of identification of web sites is based on the usage of special features of the web site, like the payment method.

In the 'follow the money' approach, EUROPOL has successfully identified a large number of websites selling counterfeit products (EUROPOLMONEY 2015).

For *machine-based*, various techniques can be used for identifying phony websites. Automated detection systems have emerged as a mechanism for combating fake websites, however most are fairly simplistic in terms of their fraud cues and detection methods employed as described in (Abbasi (2010)). Consequently, existing systems are susceptible to the myriad of obfuscation tactics used by fraudsters, resulting in highly ineffective fake website detection performance.

The following main techniques for machine-based approach can be used:

1. Lookup mechanisms try to identify phony websites by looking up to blacklists comprised of uniform resource locators (URLs) taken from member-reporting databases maintained by online trading communities. Note that the reliance by these systems on people's reports makes them reactive by nature: by the time fake websites are added to the blacklist, many users have already been exposed to them (Chou et al. 2004).
2. Classifier systems detect fake websites based on the appearance of fraud cues in website content and/or domain registration information. Many fraud cues or simply features of the web site can be used to classify and detect fake website: specific sentences are often used in web sites, grammar errors or typos, lengthier URLs, and ones with dashes or digits are also common in fake websites. Fake e-commerce websites also copy company logos from the websites they are mimicking. The main challenges for classifier systems are the choices of the features and the fact that fake websites can be periodically be updated and made more sophisticated, so that the previous techniques are not valid any longer in a subsequence check. More sophisticated analysis techniques based on statistical learning or statistical classifiers can also be used (Abbasi (2010)), but again the choice of the features is essential to decrease the rate of false alarms. Another approach used for fake medical web sites is described in (Abbasi (2012)), where an adaptive learning algorithm called recursive trust labeling (RTL) was used. RTL uses underlying content and graph-based classifiers, coupled with a recursive labeling mechanism, for enhanced detection of fake medical Web sites.

The greatest issues of the human based approaches is that a) they require considerable resources to collect and analyse the reports and investigate manually the reported web sites and b) they are able to control only a portion of the web sites in the market. In addition, the reports should be kept confidential to avoid image impacts to rightful e-commerce web sites.

The greatest issue for machine-based approach is the high percentage of false alarms and the fact that fake e-commerce web sites continuously evolve and become more sophisticated so it become a race between designer of fake web sites and analysis tools to identify them.

Probably, the most effective way forward would be a combination of the human-based or machine-based approaches, where machine-based techniques use the detected and recorded web site to build a database of statistical significant features, which can be used to identify additional fake web sites. There are various examples of systems, which use a combined approach. For example, (CTECH 2015) uses an approach based on images provided by customers. Another example is (NETNAMES 2015).

Another important weapon is increased awareness for customers. A detailed and updated list of specific features of web sites and counterfeit products (e.g., low quality logos) sold on the web can be quite useful to inform customers of the potential presence of counterfeit products. See

http://www.stopfakes.gov/sites/default/files/Consumer_Tips.pdf for an example of the awareness tool, which can be proposed.

7.1.3. Web blogs or social network websites

Similar techniques to what described in the Fake Websites can be used. In addition, another teqnique can be based on the analysis of the level of trust of social network websites, where a low level of trust can indicate a social network website, which is involved in non-compliant practices. A study on the application of trust model in social networks is provided in (Guo, 2011). While, this technique is still very much in a research phase, the possibility of quantifying with a level of trust a specific fake site could be helpful to differentiate social networks websites. Trust can be built using different features or metrics of the website like number of positive or negative feedbacks, items on sale, type of information provided and associations to other social network websites. In other words, if a social network is not associated to a trusted association or web site (e.g., an alternative medicine blog is not associated to a medical foundation or an university), this can suggest that the social network website is not to be trusted or trusted to a limited level.

7.1.4. Proper e-commerce retailers including auction sites

In this case, the previous techniques used for the fake web site or the social network website selling counterfeit items do not apply because the e-commerce web site is a valid one. What is required in this case is a greater control on the supply chain and the relationships with supplier and rights holders to avoid that counterfeit goods enters in the distribution chain.

The role of Due Diligence and Responsible Supply Chain Management for the fight against counterfeiting and IPR infringement has been evaluated in (EC 2015) where e-commerce is a specific scenario.

Due Diligence techniques applied to e-commerce can be classified in three main areas:

1. Definition of Traceability policies, which have the objective of identifying the history, distribution, location and application of products, parts and materials, to ensure the reliability of sustainability claims. By implementing traceability of the goods, the e-commerce company can mitigate the risk of counterfeiting goods entering in the chain by preventing their entry or by identifying them when a notification of counterfeit good has been created.
2. Design of policies with suppliers to implement control and collaboration with their suppliers in order to identify root-causes and take corrective actions whenever a violation is identified. Such policies can include service level agreements between the e-commerce companies and the suppliers. Integration and alignment between the company and its supply chain is important for sharing responsibilities, information and risks, for setting goals, for exchanging feedbacks on performance and for laying the foundations of risks prevention. A *transparent and open communication* is part and parcel of such collaborative approach.
3. Communication channels with the right holders of the goods. The right holders can establish procedures to notify the e-commerce platforms, which offers of sale concern counterfeit products or which sellers are offering counterfeit products for sale. In this case, the e-commerce platforms must set-up information channels to the right holders. In one direction, the right holders shall report to the e-commerce platform the presence of counterfeit goods on their web-sites. In the other direction, the e-commerce platforms will notify the right-holders on the successful removal of counterfeit goods.

In addition, another information channel is from the consumers themselves to the e-commerce platforms. Consumer complaints on the received counterfeit goods can be forwarded to the rights holders from the e-commerce platforms. Many e-commerce

platforms have usually implemented this technique (e.g., see (EBAY 2015)). A communication channel should also be established from the ecommerce platform and the rights holder. In this channel the ecommerce platform informs the rights holder of sellers who go over a predefined sales level in a given period. The rights holder can then be given the opportunity to confirm whether the products being sold are genuine or fake.

7.1.5. Analysis of the detection of non-trustable e-Commerce web sites selling counterfeit goods

In the e-commerce word, many authentication techniques based on the visual inspection of the analysis of the physical features of the good cannot be applied by the consumer because the web site only provides an image and description of the good, which may not even related to the good itself. Other techniques must be identified. In the previous section, we have identified three main sub-cases of the counterfeiting problem in e-commerce. Each sub-case may require the application of different techniques. For proper e-commerce platforms and web site, the risk of counterfeiting products can be mitigated by Due Diligence and Responsible supply chain management processes to increase the control on the supply chain and the relationships with the supplier. In some cases, such practices are already being defined by the main e-commerce company. In the cases of faked web-sites, various techniques are available from the simple reporting by customers or law enforcers to sophisticated analysis algorithms based on the features of the fake web site. While some of these algorithms are still in the research domain, some private companies have started to implement them in the market. The third sub-case of social networks is more recent and more challenging because such web sites are more difficult to identify. Even if techniques based on trust have been described in research literature, their applicability in the market is limited at the moment.

7.2. Application of Internet of Things (IoT) to fight against counterfeiting

7.2.1. Description of the technique

The Internet of Things (IoT) is a concept being increasingly supported by various stakeholders and market forces. The idea is to connect various devices or objects ("things") through wireless and wired connections and unique addressing schemes and create a pervasive environment where a person can interact at any time with the digital world and physical world. IoT technologies are heavily dependent on the clear identification of the "thing" or on the possibility to acquire information on the environment and other objects through sensors. With these two capabilities, IoT can become a new technique for tracing and tracking goods in supply chains, as well as verifying product authenticity.

The capability of IoT to improve track and trace for fight against counterfeiting has also been recently highlighted in (MICROSOFT 2014), where it was said that IoT can improve product serialization to help companies protecting their brand by making counterfeiting very difficult. Another example is from the Johnny & Walker company for the tracking of bottles (see (Walker 2015)).

As described in (Li (2013)), IoT can be considered as an applicable new technique for tracing and tracking goods in supply chains, as well as verifying product authenticity. The advantage of the pervasive connectivity of IoT may mitigate the risk of imitating product series numbers or phony packaging, because the authentication information associated to a RFID or bar-code could be checked to a remote server.

In (Xu, L. (2011b)), the author describes the application and the role of new technologies like service-oriented architecture (SOA), RFID, agent, workflow management, and the Internet of Things (IoT) to enable real-time quality management and control in the supply chain. The paper attempts to analyse the current state of the art in information management for supply chain quality management, reviewing the current research and development in information architecture for supply chain quality management, and highlighting some of the key technologies that have the potential to significantly improve the performance of supply chain quality management. Unfortunately, a cost/benefit analysis is missing in the paper.

Another example is provided in (Li et al (2102), which describe the integration of wireless networks with cloud infrastructure. The implementation of algorithms and databases to collect the data collected in the field (e.g., RFID or barcode) could deployed in cloud infrastructures, which have more capable processing capabilities than a mobile device. A cost/benefit is also missing in this paper but it is highlighted that the development of new applications (e.g., against Counterfeit) could be implemented and deployed as an add-on on existing infrastructures rather than creating a new infrastructure.

7.2.2. Analysis on the Application of Internet of Things (IoT) to fight against counterfeiting

The concept of IoT is a natural extension of existing ICT technologies with greater wireless connectivity, remote server capabilities (e.g., cloud computing), improved track and trace granularity and so on. From this point of view, existing anti-counterfeiting technologies (e.g., Track and Trace) can exploit new IoT technologies. In other words, IoT is not going to be revolutionary approach to the fight against counterfeiting but rather an evolutionary approach.

While the concepts of IoT for fight against counterfeiting has many promises, there are not many products in the market at this moment. This is sign that related products are still at an early stage.

Finally, because the application of IoT to the fight against Counterfeit is a concept strictly related to the Empowerment of the customer, when the customer is capable to access IoT products and services, we refer to section 12. Empowering the Consumer for a follow up of the analysis (including cost/benefits considerations).

7.3. Correlation of data from difference elements/sources

7.3.1. Description of the technique

In this category, we have all the solutions where data is correlated from different sources to identify a counterfeit product. One example is the correlation from different points of a supply chain as described in Dada et al., (2008), where counterfeits are detected in an RFID enabled supply chain using proximity information of items that can be gathered. In a similar way, data from different parts of the supply chain can be analysed using data mining technologies as described in (Lee (2013)), where supply chain patterns from trace records and a classification algorithm is used to identify the potential introduction of counterfeit products.

The use of analytics tools to fight against counterfeiting by aggregating different types of data has been also proposed by the U.S. Intellectual Property Enforcement Coordinator 2013. Joint Strategic Plan On Intellectual Property Enforcement in USIPEC (2013).

In a similar way, the authors in Pouwan et al, (2005) show how businesses can protect their products from counterfeiting by using a secure mobile track and trace system,

which will allow their stakeholders to authenticate the products in real time through a web enabled mobile camera phone.

7.3.2. Analysis on correlation of data from difference elements/sources

The techniques of correlating data from different sources could be quite effective especially, when it is used in combination with track and trace systems. Analytical tools can detect anomalies in the supply chain and report them. From this point of view, analytical tools can be also complement Responsible Supply Chain Management (RSCM) responsibility because they can implement checks that the RSCM "controls in place" are effectively working.

The costs associated to the analytical tools are related to the implementation of the collection and processing of data from different sources. Collection points must be set in specific points of the supply and distribution chains. The collection points must be also periodically audited to ensure that there are no errors or failures. The implementation of the analytical tools also require domain knowledge of the supply chain and the type of products.

The collection of data can be executed with different technologies (e.g., RFID, SMS, Bar Code, QR Code, see section on 5. Track and trace techniques). As a consequence, an additional cost is the parsing and harmonization of the data coming from different sources and different formats.

8. Organizational and procedural aspects and techniques

The aim of this section is to discuss the organization and processes aspects for the application and deployment of the authentication technologies.

Technologies can be effective only if they are applied correctly with organization frameworks both existing or to be defined. As described in (Chaudhry (2009)), a multi-pronged approach is needed. For example, existing approaches on supply chain management already existing in the company can be complemented by authentication technologies at critical points of the supply chain.

Here we identify the main organizational and processes, which can be used together with authentication/track trace techniques or on their own.

8.1. Due Diligence and Supply Chain Management Responsibility

Due diligence practices are another powerful tool to mitigate risk of counterfeiting or IPR infringement. Due diligence practices for the relationships with second or third tier suppliers can prevent the introduction of counterfeit products in the supply chain of the main manufacturers/producers. In another area, due diligence can also mitigate the risk of counterfeit products due to overproduction where sub-contracting manufacturers produce and sell components in addition to the ones requested by the main company.

Organizational aspects are also important in the effectiveness of solutions for fight against counterfeiting based on track and trace and the involvement of the end-users, which can be a law enforcer or a generic consumer (see also section 12. Empowering the Consumer). If the supply chain of the producer is a closed-loop, the tracking data of a product will not be available outside the producer context. As a consequence, a consumer would not be able to use it to determine the authenticity of a product. Then, a recommendation would be to provide open-loop supply chain or implement a system (e.g., gateway) to distribute the tracking data to the end-users.

Additional details on the application of Due Diligence and Supply Chain Management Responsibility procedures to fight against counterfeiting and IPR infringement is provided in technical report (EC 2015), which also provides recommendation on the application of such procedures.

8.2. Informing consumers/Awareness

As described in (Wilcock 2013), consumers are not very educated about the ramifications associated with counterfeiting (L. Lipkus, personal communication, 2012). Even if they are aware of the potential consequences of buying counterfeit products both from a financial impact on the society and from a safety point of view (e.g., fake medicines), the economic drivers (e.g., cheaper fake products than the real ones) are very strong as reported in (PWC 2013). Education programs that address the varied motivations of consumers need to be developed and appropriately disseminated. For example, while it is known that low income consumers purchase counterfeit products because of price incentives, this information may be insufficient to define an anti-counterfeiting strategy. Anti-counterfeiting programs need to emphasize quality and safety and reinforce the value of the authentic product. They should be tailored to the country for which they are designed in order to address specific beliefs and ethical norms prevalent within the society.

Additional consumer-based strategies should also be considered. Since satisfied consumers are more resistant to changing their subsequent behaviour, legitimate

businesses may consider offering consumers incentives that strengthen the relationship not only with the product but also with the firm itself.

8.3. Harmonization of customs procedure

Customs procedures in different parts of the world may share a common approach but the specific procedures are different. Considering that counterfeiting is global problem, the harmonization of customs procedures could enhance the fight against counterfeiting. The process for harmonization of the customs procedures started already many years ago with the Kyoto Convention, adopted in 1973, revised in 1999 and entered into force in February 2006. The World Customs Organization is actively working in this area with the definition of the SAFE Framework of Standards, whose objectives include the strengthening of networking arrangements between customs administrations to improve their capability to detect high-risk consignments (like counterfeit products).

8.4. Establishing notification channels for end-users

Another powerful technique to mitigate counterfeiting is to establish notification channels from end-users, which can notify the brand-owner, the manufacturer or the distributor on the presence of counterfeit products. One example is the complaint channel, where complaints can also be used to notify the reception of counterfeit items (see (EBAY (2015)).

There are also web-sites either privately or publicly funded where a consumer can report a counterfeit items or a web site. An example of private funded web site is TLAND (2015), where on the Timberland website, consumer can report counterfeit Timberland products. An example of a public funded (US government) is USSTOPFAKES (2015), where consumers can report both counterfeit products and counterfeit web sites.

One issue with the notification by consumer is that consumer themselves may not have strong drivers to notify counterfeit products because of the fear that they will be fined or exposed. Special incentives could be applied to drive the consumer to report on counterfeit goods. An example is the uFaker application UFAKER (2015), which allows a consumer to report fake products in exchange for online discounts. These reports are then entered into a database, which companies can mine to determine where to target their investigations.

9. Government and Private Initiatives

The aim of this section is to provide a brief description of the main government and private (association of companies) initiatives for the fight against counterfeiting and IPR infringement. The list is not exhaustive as many countries around the world have programs to fight against counterfeiting.

9.1. World Customs Organization and IPM Connected

IPM Connected by the WCO is one of the largest and most effective implementation of technical means to fight against counterfeiting.

In 2014, IPM connected had around 80 countries and 8000 customs officers organizations connected to the application.

As described in (WCO 2015), IPM addresses two main goals:

1. the possibility to use mobile devices to scan barcodes found on millions of products
2. the possibility to interface IPM with authentication and traceability solutions companies.

IPM connected can be quite useful for customs officers. Custom officers scan the barcode on a product and if the product is secured by a track&trace or authentication solution, IPM automatically launches the application, allowing them to instantly verify the authenticity of the product.

The main authentication technology currently used by IPM Connected is the checking of the barcode. From the initial version available through a fixed computer (e.g.,) (IPMv1), a new application on mobile devices was made available in 2013 ((IPMv2). A third version of IPM connected (IPV3) does not only allow Customs officers to control physical products but does also provide them with enhanced traceability of the international supply chains. The scanned barcode is sent to a remote server, which provides back information on the product itself to identify genuine from fake products: technical description, image and video, examples of genuine/fake, packaging information, routes, previous cases and right holder's contact details.

The application allows searching of products on the basis of names or other information. The Custom officer requests are geo-tagged to provide the location where the customs officer request and the potential identification of a fake product is executed. An important feature of IPM connect is the capability to access routes taken by genuine products to distinguish them from fake products. In addition, IPM connect can provide examples of counterfeits or packaging information like images of counterfeit products to support the customs officer in the identification of counterfeit goods.

Additional details are in (WCO 2015).

9.2. Business Action to Stop Counterfeiting and Piracy (BASCAP)

In 2004, ICC launched the Business Action to Stop Counterfeiting and Piracy (BASCAP) to combat product counterfeiting and copyright piracy worldwide.

The goal of BASCAP was to bring firms together to pursue a more unified approach to combating counterfeiting and piracy. Its efforts include the creation of platforms for exchanging information on the counterfeiting and piracy situation in different economies and sectors, and for sharing information on effective brand protection techniques. Research projects have been funded to investigate effective methods to fight against counterfeiting in different nations. BASCAP produced a very relevant global survey on counterfeiting and piracy in 2007 (BASCAP 2007), which revealed that industry efforts have mainly focused on initiatives to develop technologies to combat infringement and that resources have also been directed to aiding enforcement and improvising awareness, but to a lesser extent.

A more recent report (BASCAP 2015) has highlighted the important development in the counterfeit phenomenon in the world. Key findings of the report are:

- The growing important of Online marketplaces. For physical items, counterfeiters infiltrate both large and small commercial exchanges on e-commerce sites. In blurring the distinction between real and fake products, they succeed in selling staggering quantities of infringing items.
- Deploy technologies, such as tracking and tracing, where possible, to complement monitoring and compliance efforts, basing them on open standards to ensure interoperability between systems and to avoid fragmentation across companies, sectors and countries.
- Support the deployment of Due Diligence schemes with suppliers to have a better control on the supply chain and avoid the inflow of counterfeit products.
- Improve tracking in container shipping.

9.3. Anti-Counterfeiting Trade Agreement (ACTA)

Anti-Counterfeiting Trade Agreement (ACTA) is a multinational treaty for the purpose of establishing international standards for intellectual property rights enforcement. ACTA includes articles on Enforcement Practices, International Cooperation, Civil Enforcement and Border Measures.

Some aspects of ACTA have been criticized and it has been rejected by the European Parliament in 2012 (http://www.europarl.europa.eu/news/en/news-room/content/20120703IPR48247/html/European-Parliament-rejects-ACTA).

9.4. Office for Harmonization in the Internal Market (OHIM) and European Observatory on Infringements of Intellectual Property Rights.

The European Observatory on Infringements of Intellectual Property Rights is a network of experts and specialist stakeholders, whose objectives are to (from OHIM (2015)):

- Provide evidence-based contributions and data to enable EU policymakers to shape effective IP enforcement policies and to support innovation and creativity
- Provide data, tools and databases to support the fight against IP infringement

- Provide knowledge and learning programmes for IP and enforcement authorities as well as for businesses and IP practitioners
- Develop initiatives to help innovators, creators and businesses (especially SMEs) protect their IP rights
- Design campaigns to raise awareness of the value of IP and the negative consequences of IP infringement

The Observatory is coordinated by the Office for Harmonization in the Internal Market (OHIM), which has the task to promote and manage Community Trade Marks and Community Designs within the European Union. It carries out registration procedures for titles to EU industrial property and keeps public registers of these titles. It shares with the courts in Member States of the European Union the task of pronouncing judgment on requests for invalidation of registered titles.

10. Comparison Matrix

10.1. Introduction

The purpose of the comparison matrixes is to show how the different techniques can be used in the different domains.

10.2. Metrics

The following evaluation metrics will be used to compare the different technologies against the use cases. The evaluation metrics are all positive to facilitate the analysis in the comparison matrixes.

1. **Technical simplicity:** This metric is used to determine the complexity of the technical solutions from the point of view of design and deployment. For example, a bar code is simpler than a sophisticated covert token. The antonym of complexity is used in the matrix to have a positive evaluation metric.
2. **Field Identification.** This metric is used to evaluate how complex is to identification of the goods in the field. It is measured as a positive metric, which means that an higher value means a low level of complexity and cost of the identification device/facility or laboratory. For example a bar code has an high value of field identification while a sophisticated technique like X-Ray, which requires an expensive forensics lab has a low value of field identification. This metric is used to identify the techniques, which can support the empowerment of the consumer.
3. **Accuracy.** This metric is used to evaluate the accuracy of the technology to detect a counterfeited product. For example, how FTIR can be accurate to detected counterfeited textiles. Note that accuracy could be impacted by the risk of clonability. If the authentication information can be easily cloned, this will produce a low score for accuracy.
4. **Impact to the good (opposite of destructiveness):** This metric is used to indicate when a test is destructive: if the good under inspection will be destructed after the test.
5. **Economic efficiency:** This metric is used to evaluate the cost of implementing and deploying the technology. For example, spectroscopy could be quite accurate and effective but it may very expensive to apply. The antonym of cost is used in the matrix to have a positive evaluation metric.
6. **Extendibility:** This metric is used to evaluate the future extendibility of the technology. For example, if RFID technology can be enhanced in the future to support dynamic re-configurability. This metric is opposed to technological obsolescence.
7. **Adaptability to organizations and existing processes:** This metric is used to evaluate the impact of the option to organizations and existing process. For example, if the adoption of the new technology requires the implementation of new complex processes, this could be a negative factor.
8. **Market support.** This metric is used to evaluate the market support by the stakeholders. A technology can have benefits but it may not be adopted by the market if it is mostly a proprietary solution or too complex or costly to implement and deploy.

9. **Level of Training.** This metric is used to evaluate the level of training needed. It is measured as a positive metric. An higher value means a low level of training.
10. **Technical maturity.** This metric is used to evaluate the maturity of a specific technique. Some techniques like RFID are already well adopted in the market while other are still in the research phase.

The metrics are positive, which means that a technique with higher value is more feasible for a specific domain.

10.3. Comparison Matrixes

In the comparison matrixes a value from 1 to 5 is used to evaluate the relevance of the metric, with 5 the highest value and 1 the lowest value. In the evaluation, we do not use No-Go options with the meaning that even a low score does not preclude its use in a specific domain.

Note that the single techniques are evaluated. The combination of different techniques can be more effective than a single techniques. For specific cases, this evaluation can be executed in a second phase.

	Description
1	This is the lowest score. This indicates that the proposed technique is not really applicable or feasible. For example, the cost or the technical complexity of implementing a specific solutions is very high.
2	This score indicates that the proposed technique supports the metric in a very limited way. For example, market support is weak (e.g., very few products) but present, which could mean that we are in the early phase of technological adoption.
3	This score indicates that the technique under analysis partially satisfies the metric. For example, the technique is valid but counterfeiters have already identified new sophisticated means to cheat the technique.
4	This score indicates that the technique under analysis satisfies the metric to an high degree. For example, the technique is very cost effective.
5	This score indicates that the technique under analysis satisfies the metric to an excellent degree. For example, the accuracy of identification a fake good is extremely high on a statistical basis (e.g., 99 %).

Figure 18 Values for the evaluation of the techniques

A value of 0 means that the technique is not applicable. For example, unintentional radio frequency emissions does not apply to textiles, which do not generate radio frequency emissions.

10.3.1. Evaluation Matrix

The following link in this section points to the excel file, which the evaluation matrix of the different techniques.

The evaluation matrix is a qualitative analysis, with the objective to provide hints on the feasibility of a technique in a specific domain. The analysis is based on feedback from

experts in the fields, manufacturers of anti-counterfeiting solutions and the references used in this report. New products coming into the market or new technological evolutions could alter some of the values in the matrixes in the short and medium term.

The following link points put to the excel file containing the analysis, which will open if you read the report as word file.

If you read the report as a PDF file, the analysis is also provided in Annex 1 as a list of separate tables for each domain.

analysis_technique_v7.xlsx

11. Forecasting new threats for fight against counterfeiting

In this section, we describe future potential threats in the fight against counterfeiting. As described in the rest of the report, fight against the production and distribution of counterfeit products is often a never-ending battle between companies developing anti-counterfeit technologies and the counterfeiter themselves.

We identify the following threats:

- 3-D printing

One example of new technologies, which could support the counterfeiting phenomenon is 3D printing as described in (WIRED 2015). The article claims that the "threat of a major surge in counterfeiting based on the availability of relatively cheap 3D printers, increasingly sophisticated printing materials, and a never-ending supply of CAD designs available on the Internet will fuel an enormous black market in counterfeit parts" Along the same lines, a recent report by Gartner Group speculates that intellectual property loss due to 3D printer counterfeiting could total $100 billion by 2018 (see (Gartner 2013)).

- Higher medicine costs

In recent times, new medicines with a very high price tag like SOVALDI for the treatment of Hepatitis C or Kalideko from VERTEX for the treatment of Cystic Fibrosis has been launched in the market. These drugs are just two examples of medicines for life-threatening diseases, other medicines will come in the near future. The potential for the creation and distribution of counterfeit medicines is greater when the price of the medicines is very high.

- Malicious software in electronic components and device

Most of the anti-counterfeiting techniques are focused on detecting the counterfeit good form a physical point of view (e.g., an hardware component). A new threat highlighted in (MIL (2015)) is when malicious software is inserted in an electronic component or device (e.g., a sensor). The hardware component of the electronic component or device is not counterfeit but it may be a legitimate refurbished component (and sold in this category) where malicious software is applied. In this case, the application of the overt or covert tag would not help, because it only identifies the hardware component rather than the software, which is compromised.

12. Empowering the Consumer

12.1. Introduction

This section is used to provide an overview of the main concepts of "empowering the consumer". A full detailed description of the concept is not in the scope of this report, but it is the main objective of a subsequent report, which will use the analysis of this report to select the main techniques, which can be used to empower the consumer in the detection and identification of counterfeit items.
The concept of "empowering the consumer" is not new. The need to empower the consumer to make informed choices in the market has been already presented by various sources including (EC 2011) even if the focus was not on the fight against counterfeiting but more on the detection of frauds or the protection of the customers. In addition, the ISO Strategic Plan 2011-2015 ISO (2015), recognizes that the advice and involvement of consumer stakeholders is essential to ISO's overall performance and success.
With the term empowering the individual we mean all the possible procedural and technical tools that can be available to the average buyer to protect himself from acquiring counterfeit products or to mitigate this threat. The empowerment ranges from simply avoiding being deceived and suffering economic loss to safeguarding the individual from health and life risks. These tools are not limited to a specific category. In fact, we claim that the term consumer can be used in a wider sense for the fight against counterfeiting.
Regarding the authentication techniques, empowerment of the consumer is focused on the detection phase rather than the forensic phase. In other words, the objective is to empower the consumer to detect counterfeit items through easy accessible tools and equipment (e.g., like a smartphone).
We can identify the following categories of customers:

1. The generic citizen, who wants to buy a good and would like to be empowered to understand if the good is counterfeit before the purchase.
2. The law enforcer (like the custom officer), who must detect counterfeit goods entering the border.
3. The brand-owner to detect the distribution in the market of counterfeit items.
4. Retailers/distributors which want to detect counterfeit items entering in their supply chain.
5. Enterprise, which want to buy supply material for their own business.
6. Companies which want to detect counterfeit items entering in their supply chain.

The description of techniques and the means to empower the consumer could also be of interest to other categories like regulators, consumers associations.
Under this perspective, several complementary approach directions can be followed and implemented; those approaches (and techniques) can be generally classified in "soft" and "hard".
Normally in the soft cluster fall the following approaches:

- Campaigns of awareness on the risks derived from the use of Counterfeit goods (especially effective when the target of the campaign is related to Counterfeit drugs, health devices or in general every good which, could in an explicit way put in danger the health of the consumer).
- Informative Campaigns on "visual detection" of Counterfeit goods, i.e. campaigns aiming at coaching the consumer in identifying by visual inspection the indicators which might raise some doubts on the authenticity of the good
- Create official specialized web sites that expose the methods and the associated risks from Counterfeit and counterfeit products

- Promote the use of serial numbers, barcodes, holograms and other marks to the public.

While easy to implement, soft approaches have obviously limited efficacy when the Counterfeit good is of high quality.
In this case, the detection of counterfeit products requires a certain level of expertise, dedicated devices and infrastructures. Those techniques fall into the so called "hard" cluster.
In the past only a very limited number of consumers had access to the needed expertise and resources to use hard techniques.
Today, the large diffusion of smart-phones/tables with powerful features (described below) paves the way to new anti-counterfeit detection techniques having the potential of the most sophisticated hard techniques, while guaranteeing at the same time a low cost accessibility and high usability to the citizen.
As a consequence, the focus of the empowerment of the consumer is the application of easy- accessible low cost or consumer devices (like a smartphone) or portable devices (for law enforcer), which can be used to detect counterfeit items.
While, these techniques were still considered in the research domain until few years, the lowering of the cost of technological components and the increased power of consumer devices have fostered the development of many applications for empowering the consumer.
A description of the approach for empowering the consumer is presented in Figure 19.

Figure 19 Empowering the individual

According to this vision, the centre of the new technologies to empower the citizen would be the smart-phone, as it can be considered today the natural technological everyday companion of the end-user. As such it will act as field sensor (to detect optical features, read RFID tags, geo-location etc.), telecommunication gateway (to obtain real-time information on the object or to allow direct interactions between the object and a remote verification system) and notification system (to provide information to the track and trace supply chain system)
A common smartphone is equipped today with:

1. An high resolution camera, which can be used to collect images of a good or both overt and covert tags,

2. A very powerful processing and computing platform, which is able to process sophisticated algorithms.
3. NFC readers, which can be used to read NFC tags.
4. Other sensors like magnetometers/GNSS receiver and so on.
5. Wireless connectivity through a variety of standards like Cellular networks, WiFi and so on, which can be used to connect applications or remote data servers.
6. Web browsers to access web sites.
7. Short Message Services (SMS) or Multimedia Message Services (MMS) (and future messaging systems as well)

In addition, specific add-ons, which did not exist or whose price was prohibitive until 5-10 years ago are now affordable. One example are USB Analogic Digital Converter (ADC) which cost now in the range of 10-20 Euros and which can be used to authenticate goods on the basis of their radio frequency emissions (see 4.8. Application of Radio Frequency emissions for fight against counterfeiting). The USB Visual The Augmentation system described in 4.4. Augmented Visual inspection is another example of another add-on, which can be linked/connected to a laptop/tablet or smartphone.
At the same time (as described in the previous sections of this report), anti-counterfeiting technologies, which required sophisticated laboratories and expensive equipment, are now available on portable readers and systems.
As described in the beginning of this introduction, the aim of this section is only to provide the main concepts and some examples of empowering the consumer, while a subsequent report will present in detail the main techniques and processes, which can be put in place.

12.2. Literature survey

In the following we present a short-list of technical directions the scientific community is exploring.

- Anti- Counterfeit based on Short Message Service (SMS) messages (Wang (2009)): this technique is based on the use by the citizen of SMS to query a producer database and to verify the authenticity of an object.
- Simple RFID data acquisition and online verification as from (Yan and Huang (2008)): use of different RFID tag approaches, acquisition through NFC compliant mobile phones and online verification
- Mobile track & trace systems based on QR and Bar codes as from (Lei et al. (2005)): family of techniques exploiting the presence of cameras on mobile phones to acquire QR and Bar codes and verify online their meaning/origin
- Anti-Counterfeit using reflective micro-structures as described in (Babu et al. (2010)). The concept revolves around the use of random distribution of reflective microstructures as PUF. The particles are embedded into product's surface or in the document. These particles are invisible to naked eye, the verification is done by imaging the reflections from these micro structures with a camera enabled cellphone equipped with some add-on optics.
- Community based reputation systems for anti-Counterfeit as described in (Reischach et al. (2007)): this line of work does not concentrate its attention on the mean by which detect a Counterfeit object, but on the possible ways to exploit the social network capabilities to create awareness among consumers on the presence in certain markets of Counterfeit objects. In (Reischach et al. (2007)) the authors present a system based on the use of RFID, a remote database system and smartphones for reading RFID data. The system is described as a "consumer-driven approach for product authentication", as it is based on the idea that consumers can, by scanning the RFID code, upload data about products that they discover to be counterfeited and the shop where they found them for the benefit of other consumers. On the other hand, savvy consumers can consult the database for information on counterfeits about

a product they are interested in. Although technically feasible and easy to implement, authors do not discuss issues related to the practical implications and ownership of implementing such a system.

A preliminary analysis of the literature shows how the use of mobile technologies in the anti-Counterfeit field is still at its early stage. Several technical problems needs still to be solved, from the protection of the identifying element (e.g. the RFID, the identification code, the PUF), to the definition of secure acquisition protocols (optical, radio-frequency based etc.), to the use of the data gathered (to identify Counterfeit objects, to identify malicious sellers, to disseminate awareness among consumers etc.).

Moreover, in this context we remark at the moment the lack of directives for industrial producers and other stakeholders to provide online methods for authenticity checking, which should facilitate the development and wide adoption of the techniques just described.

Along these lines, (Bilcare 2015) also underlines the potential for new smart devices to support fight against counterfeiting.

12.3. Scenarios for empowerment the consumers

We can identify two initial scenarios for the empowerment of the consumer:

1. Empowerment based on track and trace information (e.g., a barcode)
2. Empowerment based on authentication of the good on the basis of images of the good
3)

Each of these solutions has different associated implementation and deployment costs, which need to be split among the main elements of the solution:

1. Backend system
2. Database of the matching information (e.g., track and trace or fingerprinting for goods identifications)
3. Mobile applications
4. Management of the system

12.3.1. Empowerment based on track and trace information

In the first scenario, the track and trace information present on the good or the package containing the good can be checked by the consumer using the smartphone, which is connected to a remote server. The tracking information can be of different types as described in the section 5. Track and trace techniques: serial numbers, barcodes, QR code, overt and covert token containing an identification id, RFID and so on. Through a smartphone or another similar device, the consumer can read the track and trace information and send it remotely to a server, when it is compared and checked against a reference library.

This scenario already exists and tools to support the user in the validation of a good on the basis of the identification number stored in the token are already proposed by various companies. , the collection and analysis of track and trace information from the mobile device of an user has been proposed by various companies One example is the SICPATRACE system (SICPA 2015) already presented in the previous sections, which can be used by a generic user or a retailed to check the validity of a good. Another well know example is the IPM Connected program from WCO described in section 9. Government and Private Initiatives. An example based on RFID/NFC is from FINNCODE (2015). We can conclude that this technique is quite mature and it is a primary candidate for empowering the consumer in the fight against counterfeiting.

From a business/cost point of view the empowerment must be built on an existing infrastructure as the library of the good identifiers must be built by the manufacturers or the retailers. Then, the empowerment is mostly an extension of existing and already deployed track and trace infrastructures. This means that the business costs can be very high or very low on the basis of the presence of the existing track and trace

infrastructures. The approach of using the same track and trace infrastructure already developed by the manufacturers and retailers for the end-users as well is also proposed by NXP[3], one of the largest manufactures of RFID.
Even if an existing supply chain infrastructure is already present, the tracking and tracing data may not be available to the consumer or to an application to empower the consumer. In this case, we have to distinguish between close-loop track and trace supply chains. A *closed-loop* supply chain is where the manufacturer, retailer and distributor are the same entity and the tracked goods are controlled by the same business entity (either directly or indirectly). An *open-loop* supply chain is instead where the tracked goods can be distributed to different business entities, each of them equipped with its own back-end. This difference is quite relevant to support the empowerment concept because in the closed-loop, the ICT infrastructure is not designed to share information on the tracked goods with external entities. In the open-loop, the extension to the end-user is relatively straightforward and the associated costs are similar to the implementation of an android application, connected to a remote backend infrastructure (e.g., a cloud infrastructure), which can range from tens of thousands of euros to hundreds of thousands of euros.
Another aspect to be considered for the development of an empowerment solution is related to information sharing among the different back-end systems, which store the tracking information on the goods. The back-end systems should be capable of exchanging information with similar data formats. In addition, security and access control solutions should be developed to protect sensitive data but also to guarantee access to the end-users or the empowerment back-end systems, which are responsible for matching the information collected by the end-users. All these factors contribute to the overall cost of the empowerment solution.
To conclude, it is not possible a-priori to provide a generic cost for the implementation/development of an empowerment solutions based on track and trace systems. We can identify the following main drivers for implementation costs:

1. *Open Loop against Closed Loop supply chain*. If the empowerment solution must be built on a closed loop chain, this will require extensive and costly modifications to the supply chain. This is not the case of an open-loop chain, which is designed to support different entities.
2. *Integration of back-end system from the data format point of view*. The back-end systems used to support the supply chain should be interoperable and use a similar data format (e.g., based on an OASIS standard).
3. *Access contro*l. The access to data of the track and trace supply chain should be regulated but also able to support the empowerment solution.
4. *Design and implementation of the mobile device application*. This cost is relatively minor in the case of track and trace based on simple overt and covert techniques because an application on a smartphone can implement that.

12.3.2. Collection and analysis of images of the object to be authenticated

In this solution, the user collects an image of the object to be authenticated and use algorithms to provide an estimate that the image is related to a valid (non-counterfeit) good.
An example of this solution has been announced recently by NEC in (PCWORLD, 2014). The electronics maker NEC has developed an authentication system that compares images taken with a phone with those in a cloud-based database. Images of the authentic product from the manufacturer would need to be registered beforehand. As described in the report, this can be applied to the retail sector or any other good, which can be identified through augmented visual inspection.

[3] http://www.nxp.com/applications/rf-identification/fmcg.html#design-considerations

NEC notified that the technology is currently in the testing phase and the firm plans to release a commercial version in 2015.
The article points out that "object fingerprint authentication technology" is the first such system in the world that can identify individual objects, according to the company.
The know-how makes use of fine patterns in the grain of metal or plastic that occur naturally during manufacturing and are invisible to the human eye.
The system can be used to find pirated goods, to trace the origin and distribution through the marketplace of authentic goods and to manage components in industrial applications such as maintenance and repair work, making sure they're being used correctly.
This is an example of the technical and commercial feasibility of the empowerment application at least based on images.
In comparison to the solution 1), the effort (in terms of development of the solution) can be much larger for the following reasons:

1. Existing track and trace infrastructures cannot be reused for this solution, which is based on the identification of images of the goods. In most cases, a new infrastructure must be put in place. In the example of NEC, a Cloud infrastructure must be put in place to store the fingerprints of the existing goods.

2. There may be a large variety of goods, where we need to collect the fingerprints, which are used for pattern matching. The collection of fingerprints can be quite complex and effort-consuming because the good should be photographed in various positions and angles. In addition, a retail or apparel manufacturer can produce different types of products at different time, so the database must be continuously updated.

3. The delivery of images from the mobile phone must be supported by high speed wireless connection. The high speed is needed because the higher the quality of the images and the higher the accuracy of the algorithm. While, this may not be a problem in the future, there are still many areas today, which provide limited data connectivity.

An additional issue of this solution is that techniques of pattern matching based on the images of dress and apparel can lead to false alarms due to damages in the fabric of the good, different light conditions and so on. There is an extensive literature on pattern matching of images, which identify the main challenges for accurate identification. See for example (Rytter, W. (2000)).
To conclude, we can identify the main drivers for the implementation and deployment cost of this solution:

1. *Remote database*. A back-end database (e.g., Cloud Computing) should be created with all the fingerprint of the goods to be checked for Counterfeiting.
2. *Implementation of the algorithms*: Sophisticated algorithms for pattern matching should be implemented. The algorithms should be optimized for the type of good.
3. *Fingerprints collection*: Fingerprints should be collected for each type of good produced by a manufacturer.
4. *Cameras with adequate resolution*: mobile devices (e.g., smartphones) of the user should be equipped with cameras with adequate resolution to support the image validation. This should not be a problem in the future, as the level of resolution of the camera in commercial smartphone is increasing.
5. *Data connectivity*. User should have access to high speed wireless data link to support the upload of images to the central cloud. Note that existing wireless communication standards are usually asymmetric: the uplink capacity is usually less than the downlink capacity for business reasons as the majority of the traffic is usually in the downlink direction.

12.3.2. Conclusions on Analysis on empowerment for fight against Counterfeiting

In table, we provide a comparison of the three techniques from the cost, maturity and complexity point of view:

Table 2 Comparison of the techniques to empower the consumer

Technique	Cost in the back-End/Infrastructure	Cost for the user	Maturity
Collection of track and trace information	Low if the solution is based on an extension of an existing *open-loop* RFID track and trace infrastructure Medium if the solution is based on an extension of an existing *closed-loop* RFID track and trace infrastructure Very high is a new RFID track and trace infrastructure must be created.	Low, because RFID readers are widely available and they can be easily installed in mobile devices. Needed data connectivity is limited.	High, because solutions are already available.
Collection and analysis of images of the object to be authenticated	Medium-High because infrastructures are not developed yet. On the other side of the coin, there is only data collection point to be created in the manufacturing process.	Low because most of the mobile devices have a camera with high resolutions (more than 5 MPixel). Data connectivity should be available.	Medium. NEC has announced a solution available to customers in 2016. (PC World, (2014)).

12.3. Privacy aspects

This section addresses the problem of the privacy of the individual. The technologies used to identify a good could also become a privacy risk because tracking information of the good can be captured and processed. For example, and active RFID on a package containing medicines for diabetes could be read from a distance. In another case, the RFID information on a luxury bag could be read from a distance, exposing the owner or carrier of the bag to the risk of theft. Various techniques to mitigate privacy risks and they are described in the JRC report (JRC 2012), which analysed in detail the privacy risks associated to the use of RFID and the potential countermeasures. Here we focus on RFID because most of the other track and trace technologies do not use radio frequency emissions and the collection of tracking data must be implemented at a visual distance. Then, the owner of the good is obviously aware that somebody is trying to collect the identifier information.
Another privacy risks related to empowerment the consumer is that the consumer (through the application in the smartphone) must transmit the identifier information to a remote server on the good, s(he) want to check. Transmitted data can include the identifier of the consumer, which is considered personal data. On the other side of the

coin, it can be claimed that the consumer is willingly providing this information and has provided his/her informed consent to the use of such data to support the fight against counterfeiting. Another approach could be to limit or remove the personal data used in the validation of the good. In other words, the personal data sent to the remote server could be made anonymous or pseudonyms could be used. After all, the application for empowering the user is designed to identify and validate the good rather than the consumer.

To summarize, the dangers of privacy risks in "empowering the consumer" are limited either because the consumer has provided an informed consent or because privacy mitigation technologies could be put in place

13. Recommendations

In this section, we identify recommendations, which are based on the analysis of this report and the feedback from experts.

1. Due Diligence and Responsible Supply Chain Management techniques can be quite helpful to mitigate the risk of production and distribution of counterfeit items both for manufacturers and retailers. In particular, these techniques can be applied to large e-commerce companies to ensure that the products sold on their web-sites are not counterfeit. The organizational and financial costs for the application of Due Diligence and Responsible Supply Chain Management techniques to small companies must be carefully evaluated.

   Recommendation 1) The application of Due Diligence and Responsible Supply Chain Management to e-commerce distribution should be further analysed and the definition of a suitable regulatory framework should be supported.

2. The evolution of technologies for forensic analysis has considerably decreased the costs of tools and equipment to implement and deploy these technologies. In this context, many techniques previously available only in the forensic labs can be implemented in cost-effective portable equipment which can be used by law enforcers or even generic citizens.

   Recommendation 2) The application of techniques for forensic analysis to empower law enforcers or even the generic citizen in the field in the fight against counterfeiting should be supported in collaboration with industry and standardization bodies.

3. The capabilities of consumer equipment like smartphones has greatly increased in recent times. The availability of wireless connectivity and high resolutions cameras can be used to support the fight against counterfeiting even by the generic citizen. Awareness on counterfeit products can be made accessible to the citizen through a smartphone. On the other side there are no standardization activities in this area even if there are a number of proprietary solutions appearing in the market.

   Recommendation 3) Standardization activities for the usage of consumer equipment like smartphones for fight against counterfeiting (including awareness) should be supported.

4. The technology landscape for fight against counterfeiting is quite fragmented and many private and proprietary solutions are available on the market. There is the need for a knowledge management database to be maintained and frequently updated as new solutions appear in the market. Ideally, this knowledge base should be defined at European level to harmonize the efforts for the fight against counterfeiting at European level. In addition, the knowledge management database should be linked to the techniques for empowering the consumer.

   Recommendation 4) A knowledge management database should be put in place at European level. The Office for Harmonization in the Internal Market (OHIM) and Observatory could be quite suitable to this goal.

5. As can be seen in the report, there is a huge range of possible technologies to fight against counterfeit of goods manufactured in various domains, ranging from the very simple to the highly complex, from zero cost to highly secure against compromise. The wide range of options adds to the potential security by diluting the advantage gained by a counterfeiter in defeating any one system. In addition,

brand owners are legally liable for authenticating their products. Therefore, brand owners should keep being the ones who select the technologies to apply on their products, and make this choice wisely for optimum security gain against counterfeiting.

Recommendation 5) Regulatory frameworks or guidelines should be put in place to support brand owners in their choice of selecting the best techniques for fight against counterfeiting.

6. To support the authentication of the goods in the market, manufacturers and retailers should include authentication technology in the product design, manufacturing and distribution processes. On the other side, the cost of implementing authentication technology can be quite high and it can different depending on the type of good and sectors (e.g., automotive, pharmaceutical). A cost/benefit analysis may be needed to this purpose.

   Recommendation 6) A cost/benefit analysis should be implemented for the deployment of authentication technology in the product design, manufacturing and distribution processes in different market sectors.

14. Conclusions

Counterfeiting and IPR infringement is a very complex problem, which negatively impacts not only businesses (through loss or revenues by brand owners) but also the health and the safety of the citizens (e.g., due to counterfeit medicines).
As described in the scope section, this report does not aim to address the main reasons of counterfeiting but to describe the current or potential techniques, which can be applied to mitigate the counterfeiting
Counterfeit products impact many different domains and one of the main challenges for drafting a survey in anti-counterfeiting techniques like this report is that different domains may require different techniques or that a specific technique valid in one domain requires adaption to be applied in another domain. Another challenge is that the landscape of anti-counterfeiting technologies is continuously evolving. Innovative anti-counterfeiting products and technologies appear in the market but the level of sophistication of counterfeit items also increases. A recent development is the distribution of counterfeit goods through the world wide web and e-commerce, which poses new challenges to law enforcers, customer and brand-owners. This report tried to address these developments from a high level point of view and provide a reference framework based on an extensive bibliography.
We believe that the reduction in price of consumer equipment, their increasing power and the ubiquitous connectivity can empower the consumer (where consumer is a wide category of stakeholders) to fight against counterfeiting in a more effective way than today. This topic is briefly presented in this report, but it will be the main objective of a subsequent report.

References

Lu et al. (2003). Ying Tsung Lu, Sien Chi, Compact, reliable asymmetric optical configuration for cost-effective fabrication of multiplex dot matrix hologram in anti-counterfeit applications, Optik - International Journal for Light and Electron Optics, Volume 114, Issue 4, 2003, Pages 161-167, ISSN 0030-4026.

Li (2013), Ling Li, *Technology designed to combat fakes in the global supply chain*, Business Horizons, Volume 56, Issue 2, March–April 2013, Pages 167-177, ISSN 0007-6813.

EPCIS (2014). GDSN Package Measurement Rules, GS1 Standards Document, EPC Information Services (EPCIS) Version 1.1 Specification, GS1 Standard, Version 1.1, May 2014 http://www.gs1.org/gsmp/kc/epcglobal/epcis/epcis_1_1-standard-20140520.pdf. Last accessed 30 October 2015.

CALCE University of Maryland http://www.calce.umd.edu/TSFA/part_auth_cap.htm

Griffiths, P. R., & De Haseth, J. A. (2007). Fourier transform infrared spectrometry (Vol. 171). John Wiley & Sons.

USSTOPFAKES (2015) STOPfakes.gov. http://www.stopfakes.gov/about. . Last accessed 30 October 2015

DNATech (2015). DNA technologies. http://www.dnatechnologies.com/. . Last accessed 30 October 2015.

Anshul Shrivastava, Michael H. Azarian, Carlos Morillo, Bhanu Sood, Michael Pecht, "Detection and Reliability Risks of Counterfeit Electrolytic Capacitors" IEEE TRANSACTIONS ON RELIABILITY, VOL. 63, NO. 2, JUNE 2014.

Dongwan Haa, Jeffrey Paulsenb, Nan Sunc, Yi-Qiao Songb, and Donhee Hama "Scalable NMR spectroscopy with semiconductor chips" PNAS August 19, 2014 vol. 111 no. 33 http://www.pnas.org/content/111/33/11955.full. Last accessed 30 October 2015.

Ujjwal Guin, Daniel DiMase and Mohammad Tehranipoor, "A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment" J Electron Test Jan 2014.

Dey, S., Roy, N., Xu, W., & Nelakuditi, S. (2013). Acm hotmobile 2013 poster: Leveraging imperfections of sensors for fingerprinting smartphones. *ACM SIGMOBILE Mobile Computing and Communications Review*, *17*(3), 21-22.

Bhanu Sood, Diganta Das and Michael Pecht "Screening for counterfeit electronic parts" J Mater Sci: Mater Electron (2011) 22:1511–1522.

TLAND (2015). Timberland web site. http://www.timberlandonline.co.uk/en/cs_counterfeit.html. Last accessed 30 October 2015

Walker (2015). http://www.cio.com/article/2926218/innovation/why-johnnie-walker-joined-the-internet-of-things.html. Last accessed 30 October 2015.

SPROXIL (2015). http://www.sproxil.com/. Last accessed 30 October 2015.

BRAND-I (2015). https://www.brand-i.org/. Last accessed 30 October 2015.

John M. Radman and Daniel D. Phillips, "Novel Approaches for the Detection of Counterfeit Electronic Components" Trace Laboratories Inc. October 2010.

PWC (2013). Counterfeit Goods in UK. PriceWaterHouse Coopers report https://www.pwc.co.uk/assets/pdf/anti-counterfeiting-consumer-survey-october-2013.pdf. Last accessed 30 October 2015.

MIL (2015). Counterfeit threat taking malicious turn. http://mil-embedded.com/articles/counterfeit-taking-malicious-turn. Last accessed 30 October 2015.

ADNA (2015). Applied DNA Sciences http://www.adnas.com/products/digital-dna. Last accessed 30 October 2015.

(SANCO 2013) Report prepared for DG SANCO. Research support for an informal expert group on product traceability http://ec.europa.eu/consumers/archive/safety/projects/docs/20131023_final-report_product-traceability-expert-group_en.pdf. Last accessed 30 October 2015.

Dada et al., (2008). Dada, Ali; Magerkurth, Carsten, "Anti-counterfeit Based on Supply Chain Proximity," RFID Systems and Technologies (RFID SysTech), 2008 4th European Workshop on , vol., no., pp.1,9, 10-11 June 2008.

USIPEC (2013). U.S. Intellectual Property Enforcement Coordinator 2013. Joint Strategic Plan On Intellectual Property Enforcement. https://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf. Last accessed 30 October 2015.

US Immigration and Customs Information 2015. Operation In Our Sites. http://www.ice.gov/factsheets/ipr-in-our-sites. Last accessed 30 October 2015.

DENSO (2011). QR Code® Essentials. http://www.nacs.org/LinkClick.aspx?fileticket=D1FpVAvvJuo%3D&tabid=1426&mid=4802. Last accessed 30 October 2015.

EPCGlobal (2012), The need for global standards and solutions to combat counterfeiting. White Paper by EPC Global. November 2012.

OHIM (2015). https://oami.europa.eu/ohimportal/en/web/observatory/about-us. Last accessed 30 October 2015.

NIST (2014). RFID Technology in Forensic Evidence Management: An Assessment of Barriers, Benefits, and Costs. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=916133. Last accessed 30 October 2015.

(EC 2015). European Commission, Joint Research Centre. Fight against counterfeiting of goods related to IP infringing http://publications.jrc.ec.europa.eu/repository/bitstream/JRC95089/lbna27168enn.pdf. Last accessed 30 October 2015.

NEC (2014). Contribution to ITU event on combating counterfeit and substandard ICT devices http://www.itu.int/en/ITU-T/C-I/Documents/WSHP_counterfeit/Contributions/Contribution-009-NEC-Corporation.pdf. Accessed 12 September 2015.

Gartner Group. Predicts 2014: 3D Printing at the Inflection Point

BCC Research. (2011). Anti-counterfeit packaging technologies in the global pharmaceutical and food industries. Retrieved from http://www.bccresearch.com/report/anti-counterfeit-packaging-food-fod042b.html. Last accessed 30 October 2015.

NYTIMES (2013). http://www.nytimes.com/2013/02/20/nyregion/three-men-arrested-in-scheme-to-sell-counterfeit-automotive-parts.html?_r=1. Last accessed 30 October 2015.

Filler, T., Fridrich, J., & Goljan, M. (2008, October). Using sensor pattern noise for camera model identification. In Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on (pp. 1296-1299). IEEE.

Angela Li, Yun Wei Yat, Wee Kim Yap, Chee Wei Lim, Sheot Harn Chan (2011), Discriminating authentic Nostoc flagelliforme from its counterfeits by applying alternative ED-XRF and FTIR techniques, Food Chemistry, Volume 129, Issue 2, 15 November 2011, Pages 528-532, ISSN 0308-8146.

SICPA (2015). http://www.sicpa.com/security-inks/story-security-inks. Last accessed 30 October 2015.

SAE (2015). AS6171/10. Techniques for Suspect/Counterfeit EEE Parts Detection by Thermogravimetric Analysis (TGA) Test Methods. http://standards.sae.org/wip/as6171/10/. Last accessed 30 October 2015.

Hu, C. Q., Zou, W. B., Hu, W. S., Ma, X. K., Yang, M. Z., Zhou, S. L., ... & Xue, J. (2006). Establishment of a Fast Chemical Identification System for screening of counterfeit drugs of macrolide antibiotics. Journal of pharmaceutical and biomedical analysis, 40(1), 68-74.

MICROSOFT (2014). Transform your business — and prevent counterfeiting? — with IoT https://blogs.microsoft.com/iot/2014/10/17/transform-your-business-and-prevent-counterfeiting-with-iot/. Last accessed 30 October 2015.

EUROPOLMONEY (2105). https://www.europol.europa.eu/content/292-internet-domain-names-seized-selling-counterfeit-products. Last accessed 30 October 2015.

NETNAMES (2015). http://www.netnames.com/services/online-brand-protection/ip-trademark-protection. Last accessed 30 October 2015.

UFAKER (2015). uFaker application. https://www.ufaker.com/. Last accessed 30 October 2015.

(OHIM 2013) The economic cost of IPR infringement in sports goods. https://oami.europa.eu/ohimportal/en/web/observatory/ip-infringements_sports-goods. Last accessed 30 October 2015.

(OHIM 2013b) The economic cost of IPR infringement in the clothing, footwear and accessories sector. https://oami.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/research-and-studies/ip_infringement/study2/the_economic_cost_of_IPR_infringement_in_the_clothing_footwear_and_accessories_sector_en.pdf. Last accessed 30 October 2015.

Tehranipoor, M. M., Guin, U., & Forte, D. (2015). Counterfeit Integrated Circuits: Detection and Avoidance. Springer.

Sood et al (2011). Sood, B., Das, D., & Pecht, M. (2011). Screening for counterfeit electronic parts. *Journal of Materials Science: Materials in Electronics*, *22*(10), 1511-1522.

TruTag Technologies (2015). http://www.trutags.com/trutag-platform/. Last accessed 30 October 2015.

Holzgrabe, U., & Malet-Martino, M. (2011). Analytical challenges in drug counterfeiting and falsification—The NMR approach. *Journal of pharmaceutical and biomedical analysis*, *55*(4), 679-687.

(Rako 2015). HoloTrackX™ http://www.rako-etiketten.com/en/security-technology/hologramme/track-trace-system-holo-track/covr. Last accessed 30 October 2015.

Powan et al., (2005). Pouwan Lei; Claret-Tournier, F.; Chatwin, C.; Young, R., "A secure mobile track and trace system for anti-counterfeit," *e-Technology, e-*

Commerce and e-Service, 2005. EEE '05. Proceedings. The 2005 IEEE International Conference on , vol., no., pp.686,689, 29 March-1 April 2005.

Farouk, F., Moussa, B. A., & Azzazy, H. M. E. S. (2011). Fourier transform infrared spectroscopy for in-process inspection, counterfeit detection and quality control of anti-diabetic drugs. *Journal of Spectroscopy*, *26*(4-5), 297-309.

(ATT 2015) Seal Vector. www.att-fr.com . Last Accessed 30 October 2015.

Chen et al. (2011). Chen, Y. Y., Qiu, Z. J., Lu, J. C., & Jan, J. K. (2011, October). A Secure RFID deactivation/activation mechanism for customer service and consumer shopping. In *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on* (pp. 405-410). IEEE.

(Guo, 2011). Stephen Guo, Mengqiu Wang, and Jure Leskovec. 2011. The role of social networks in online shopping: information passing, price of trust, and consumer choice. In Proceedings of the 12th ACM conference on Electronic commerce (EC '11). ACM, New York, NY, USA, 157-166. DOI=http://dx.doi.org/10.1145/1993574.1993598

Pharma IQ. (2011), How to successfully use anticounterfeiting technologies to reduce costs and increase your business value. Retrieved July 6, 2012, from http://www.pharma-iq.com/regulatory-legal/articles/how-to-successfullyuse-anti-counterfeit-techno/. Last accessed 30 October 2015.

Michael, K., & McCathie, L. (2005). The pros and cons of RFID in supply chain management. In *Mobile Business, 2005. ICMB 2005. International Conference on* (pp. 623-629). IEEE.

Olsen, B. A., Borer, M. W., Perry, F. M., & Forbes, R. A. (2002). Screening for counterfeit drugs using near-infrared spectroscopy. *Pharmaceutical technology*, *26*(6), 62-71.

Stringa et al (2010a). Innovative RFID sealing solutions for the security of supply chain Infield operational tests in Livorno harbor and Prato hub (Italy), E. Stringa, G. Azzalin, L. Faggion, F. Littmann, G. Renaldi, G. Selvagio, P. Tebaldi, JRC Technical Report JRC56368.

Bhattacharya et al (2007). Bhattacharya, M., Chu, C.-H., Mullen,T., 2007. RFID implementation in retail industry: current status, issues and challenges. In Proceedings of the Decision Science Institute Conference.Phoenix.pp.1–23.

Counterfeit Drug Forensic Investigation Network (CODFIN). Available at http://codfin.org/. Accessed 10/August/2015. Last accessed 30 October 2015.

ProofTag (2015). http://www.prooftag.net/solutions-2/authentication-technologies/. Last accessed 30 October 2015.

Scafi, S. H. F., & Pasquini, C. (2001). Identification of counterfeit drugs using near-infrared spectroscopy. *Analyst*, *126*(12), 2218-2224.

World Health Organization. Tool for visual inspection. Available: http://www.whpa.org/Toolkit_BeAware_Inspection.pdf. Last Accessed 10/August/2015.

Cassell J (2012) Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defence Industry and National Security.

Smart et al (2010). Smart, A.U., Bunduchi,R., Gerst,M., 2010. The costs of interorganizational IT innovation adoption: RFID technologies in supply networks. International Journal ofOperationsandProductionManagement 30 (4), 423–447.

Liao, Y. P., & Hsiao, C. M. (2014). A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. *Ad Hoc Networks*, *18*, 133-146.

Rogoz, D., & O'Reilly, F. (2009). Dedicated Networking Solutions for a Container Tracking System. In *Ambient Intelligence with Microsystems* (pp. 387-408). Springer US.

Stringa (2010b) Technological Solutions for an Optimized European Transport System for Freight. Elena Stringa. European Commission - Technical Report JRC62686.

Li, S., Xu, L., Wang, X., & Wang, J. (2012). Integration of hybrid wireless networks in cloud services oriented enterprise information systems. Enterprise Information Systems, 6(2), 165—187.

Simson et al (2005). Simson, L., Juels, A., & Pappu, R. (2005). RFID privacy: An overview of problems and proposed solutions.

Rizzo et al (2011), Francesco Rizzo, Marcello Barboni, Lorenzo Faggion, Graziano Azzalin, Marco Sironi, Improved security for commercial container transports using an innovative active RFID system, Journal of Network and Computer Applications, Volume 34, Issue 3, May 2011, Pages 846-852, ISSN 1084-8045.

Chong et al. (2008), Cheun Ngen Chong, Dan Jiang, Jiagang Zhang and Long Guo, Anti-counterfeit with a Random Pattern, The Second International Conference on Emerging Security Information, Systems and Technologies, 2008.

Westenberger, B. J., Ellison, C. D., Fussner, A. S., Jenney, S., Kolinski, R. E., Lipe, T. G., ... & Buhse, L. F. (2005). Quality assessment of internet pharmaceutical products using traditional and non-traditional analytical techniques. International journal of pharmaceutics, 306(1), 56-70.

Kumar, S., Kadow, B., & Lamkin, M. (2011). Challenges with the introduction of radio-frequency identification systems into a manufacturer's supply chain: A pilot study. Enterprise Information Systems, 5(2), 235—253.

WATCHES (2015). http://www.fhs.ch/eng/stopthefakes.html. Last accessed 30 October 2015.

UNODC (2014), United Nation Office on Drugs and Crime. The Illicit Traffi cking of Counterfeit Goods and Transnational Organized Crime http://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf. Last accessed 30 October 2015.

De Souza et al. (2011), De Souza, R., Goh, M., Sundarakani, B., Wai, W. T., Toh, K., & Yong, W. (2011). Return on investment calculator for RFID ecosystem of high tech company. *Computers in Industry*, *62*(8), 820-829.

Chong, C. N., Jiang, D., Zhang, J., & Guo, L. (2008). Anti-counterfeit with a random pattern. In *Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08. Second International Conference on* (pp. 146-153). IEEE.

Sheng Cao Zheng Chen Xuandong Sun, Anti-Counterfeit Authentication System of Printed Information Based on A Logic Signing Technique, Proceedings of the International Conference on Intelligent Systems and Knowledge Engineering (ISKE 2007)

Chen, Y., Mihçak, M. K., & Kirovski, D. (2005). Certifying authenticity via fiber-infused paper. *ACM SIGecom Exchanges*, *5*(3), 29-37.

(GS1 2015). http://www.gs1.org/docs/barcodes/GS1_General_Specifications.pdf. Last accessed 30 October 2015.

Warasart, M., & Kuacharoen, P. (2012, June). Paper-based Document Authentication using Digital Signature and QR Code. In *4th International Conference on Computer Engineering and Technology. International Proceedings of Computer Science and Information Technology* (Vol. 40, pp. 94-98).

Ministero dello sviluppo economico Italiano. Indagine sulla percezione dei consumatori rispetto alla contraffazione www.uibm.gov.it/attachments/indagine_percezione_contraffazione.pdf. 2014. Last accessed 30 October 2015.

Cole, P. H., & Ranasinghe, D. C. (2008). Networked RFID systems and lightweight cryptography. *London, UK: Springer. doi*, *10*, 978-3.

von Reischach, F., Michahelles, F., & Fleisch, E. (2007). Anti-counterfeit 2.0-A Consumer-Driven Approach towards Product Authentication. In *Late Breaking Results at the 9th International Conference on Ubiquitous Computing (UbiComp 2007), Austria*.

Davison, M. (2011). Pharmaceutical anti-counterfeiting: combating the real danger from fake drugs. John Wiley & Sons.

Corbellini, S., Ferraris, F., & Parvis, M. (2006, April). A cryptographic system for brand authentication and material traceability in the textile industry. In *Instrumentation and Measurement Technology Conference, 2006. IMTC 2006. Proceedings of the IEEE* (pp. 1331-1335). IEEE.

Wang, Y. (2009). Design of an anti-counterfeit system based on SMS. In *Granular Computing, 2009, GRC'09. IEEE International Conference on* (pp. 572-575). IEEE.

Liu, V., Caelli, W., Foo, E., & Russell, S. (2004). Visually sealed and digitally signed documents. In *Proceedings of the 27th Australasian conference on Computer science-Volume 26* (pp. 287-294). Australian Computer Society, Inc..

Anne E. Wilcock, Kathryn A. Boys, Reduce product counterfeiting: An integrated approach, Business Horizons, Volume 57, Issue 2, March–April 2014, Pages 279-288, ISSN 0007-6813, http://dx.doi.org/10.1016/j.bushor.2013.12.001

BSI, Technical Guideline TR-03137 (2013), Optically Verifiable Cryptographic Protection of non-electronic Documents (Digital Seal). Bundesamt für Sicherheit in der Information-stechnik (BSI), 1.0 edition, 2013.

Xu, L. (2011b). Information architecture for supply chain quality management. International Journal of Production Research, 49(1), 183—198.

NOKOMIS. (2013). Advanced Detection of Electronic Counterfeits. http://www.erai.com/CustomUploads/conference/2013/PDF/TrainingTrack11BogdanPathak.pdf. Last accessed 7 July 2015.

UNODOC (2014). Focus on the Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf. Last accessed 7 July 2015.

WHO (2008). IMPACT, Counterfeit Drugs Kill! WHO Brochure, IMPACT, 2008 http://www.who.int/impact/FinalBrochureWHA2008a.pdf (accessed 08 April 2014).

OECD (2008) OECD, The Economic Impact of Counterfeiting and Piracy, Industry, Services & Trade, 2008, pp. 1–399 ISBN 978-92-64-04551-4. (2008(10)).

KBA (2015). http://www.kba-notasys.com/. Last accessed 30 October 2015.

Seiter (2009). A. Seiter, Health and economic consequences of counterfeit drugs, Clin. Pharmacol. Ther. 85 (6) (2009) 576–578.

Weiss, A. M. (2006). Buying prescription drugs on the internet: promises and pitfalls. Cleveland Clinic journal of medicine, 73(3), 282-288.

Veronin, M. A., & Youan, B. B. C. (2004). Magic bullet gone astray: medications and the internet. Science, 305(5683), 481.

Biesman, B. S., & Patel, N. (2014). Physician alert: Beware of counterfeit medical devices. Lasers in surgery and medicine, 46(7), 528-530.

Gomez, R., & Harrison, A. (2014). Beyond Wearables: Experiences and Trends in Design of Portable Medical Devices. In *Design, User Experience, and Usability. User Experience Design Practice* (pp. 261-272). Springer International Publishing.

Reuters, (2014). Aston Martin recalls 17,590 cars due to fake parts. Reuters. http://www.cnbc.com/id/101393220#. Last accessed 2/07/2015.

GIDEP, (2006), "Agency action notice: Orange County Man Sentenced to Nearly 16 Years for Selling Subpar Flight-Critical Aircraft Parts and for Offering to Sell Fighter Plane Parts to China," Tech. Rep. AAN-U-06-018, Jan. 26, 2006.

GIDEP, (2006b), "Suspect Counterfeit CY37032P44-125AI, Microcircuit," Tech. Rep. EE-A-06-06B, Mar. 20, 2006.

Stradley et al. (2006). Stradley, J.; Karraker, D., "The Electronic Part Supply Chain and Risks of Counterfeit Parts in Defense Applications," IEEE Transactions on Components and Packaging Technologies, vol.29, no.3, pp.703,705, Sept. 2006.

Bayram, S., Sencar, H. T., Memon, N., & Avcibas, I. (2005). Source camera identification based on CFA interpolation. In *Image Processing, 2005. ICIP 2005. IEEE International Conference on* (Vol. 3, pp. III-69). IEEE.

Bayram, S., Sencar, H. T., & Memon, N. (2008). Classification of digital camera-models based on demosaicing artifacts. digital investigation, 5(1), 49-59.

Choi, K. S., Lam, E. Y., & Wong, K. K. (2006). Source camera identification by JPEG compression statistics for image forensics. In TENCON 2006. 2006 IEEE Region 10 Conference (pp. 1-4). IEEE.

Aggarwal, R., Singh, S., Roul, A. K., & Khanna, N. (2014). Cellphone identification using noise estimates from recorded audio. In Communications and Signal Processing (ICCSP), 2014 International Conference on (pp. 1218-1222). IEEE.

Garcia-Romero (2010), Garcia-Romero, D.; Espy-Wilson, C.Y., "Automatic acquisition device identification from speech recordings," Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on , vol., no., pp.1806,1809, 14-19 March 2010.

Saunders, K. M., & Berger-Walliser, G. (2011). Liability of Online Markets for Counterfeit Goods: A Comparative Analysis of Secondary Trademark Infringement in the United States and Europe, The. Nw. J. Int'l L. & Bus., 32, 37.

(OHIM, EUROPOL 2015) Situation Report on Counterfeiting in the European Union. https://oami.europa.eu/ohimportal/documents/11370/80606/2015+Situation+Report+on+Counterfeiting+in+the+EU

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker Jr, J. F. (2010). Detecting fake websites: the contribution of statistical learning theory. MIS Quarterly, 34(3), 435-461.

Chou, N., Ledesma, R., Teraguchi, Y., & Mitchell, J. C. (2004, February). Client-Side Defense Against Web-Based Identity Theft. In NDSS.

Abbasi, A., Zahedi, F., & Kaza, S. (2012). Detecting fake medical web sites using recursive trust labeling. ACM Transactions on Information Systems (TOIS), 30(4), 22.

Carbonetto, P., de Freitas, N., & Barnard, K. (2004). A statistical model for general contextual object recognition. In Computer Vision-ECCV 2004 (pp. 350-362). Springer Berlin Heidelberg.

Kovacs, S., Hawes, S. E., Maley, S. N., Mosites, E., Wong, L., & Stergachis, A. (2014). Technologies for Detecting Falsified and Substandard Drugs in Low and

Middle-Income Countries. PLoS ONE, 9(3), e90601. doi:10.1371/journal.pone.0090601.

Villasenor, J., & Tehranipoor, M. (2013). Chop shop electronics. Spectrum, IEEE, 50(10), 41-45.

DARPA technology uncovers counterfeit microchips, October 2014. http://www.networkworld.com/article/2690353/security0/darpa-technology-uncovers-counterfeit-microchips.html. Last Accessed 14/07/2015.

AERI 2015. Counterfeit Electronic Component Detection. http://www.aeri.com/counterfeit-electronic-component-detection/. Last accessed 30 October 2015.

Tzenbeisser, Stefan; Kocabas, Ünal; Rožic, Vladimir; Sadeghi, Ahmad-Reza; Verbauwhede, Ingrid; Wachsmann, Christian (2012), "PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon", Cryptographic Hardware and Embedded Systems – CHES 2012. 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings, Lecture Notes in Computer Science 7428, Springer Berlin Heidelberg, pp. 283–301, doi:10.1007/978-3-642-33027-8_17, ISBN 978-3-642-33026-1.

Devadas, S; Suh, E.; Paral, S.; Sowell, R.; Ziola, T.; Khandelwal, V., "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-counterfeit and Security Applications," RFID, 2008 IEEE International Conference on , vol., no., pp.58,64, 16-17 April 2008

Chong et al. (2008), Cheun Ngen Chong, Dan Jiang, Jiagang Zhang and Long Guo, Anti-counterfeit with a Random Pattern, The Second International Conference on Emerging Security Information, Systems and Technologies, 2008.

Chen, Y., Mihçak, M. K., & Kirovski, D. (2005). Certifying authenticity via fiber-infused paper. *ACM SIGecom Exchanges*, *5*(3), 29-37.

Warasart, M., & Kuacharoen, P. (2012, June). Paper-based Document Authentication using Digital Signature and QR Code. In *4th International Conference on Computer Engineering and Technology. International Proceedings of Computer Science and Information Technology* (Vol. 40, pp. 94-98).

Pereira, T. M., Júnior, J. A., Ortiz, R. S., Rocha, W. F., Endringer, D. C., Filgueiras, P. R., ... & Romão, W. (2014). Viagra® and Cialis® blister packaging fingerprinting using Fourier transform infrared spectroscopy (FTIR) allied with chemometric methods. Analytical Methods, 6(8), 2722-2728.

Corbellini, S., Ferraris, F., & Parvis, M. (2006). A cryptographic system for brand authentication and material traceability in the textile industry. In Instrumentation and Measurement Technology Conference, 2006. IMTC 2006. Proceedings of the IEEE (pp. 1331-1335). IEEE.

Hasse, J., Gloe, T., & Beck, M. (2013). Forensic identification of GSM mobile phones. In Proceedings of the first ACM workshop on Information hiding and multimedia security (pp. 131-140). ACM.

CTECH (2015). http://counterfeit.technology/. Last accessed 30 October 2015.

Kuemin, C., Nowack, L., Bozano, L., Spencer, N. D., & Wolf, H. (2012). Oriented Assembly of Gold Nanorods on the Single-Particle Level. Advanced Functional Materials, 22(4), 702-708.

Kotropoulos, C. L. (2014). Source phone identification using sketches of features. *Biometrics, IET*, *3*(2), 75-83.

Guin, U., Forte, D., & Tehranipoor, M. (2013). Anti-Counterfeit techniques: from design to resign. In Microprocessor Test and Verification (MTV), 2013 14th International Workshop on (pp. 89-94). IEEE.

World Health Organization. (1999). Counterfeit Drugs: Guidelines for the development of measures to combat counterfeit drugs.

BRANDSTRIKE (2015). http://www.brandstrike.com/. Last accessed 30 October 2015.

NETNAMES (2105). http://www.netnames.com/solutions/industry/luxury-brands. Last accessed 30 October 2015.

Hu, C. Q., Zou, W. B., Hu, W. S., Ma, X. K., Yang, M. Z., Zhou, S. L., & Xue, J. (2006). Establishment of a Fast Chemical Identification System for screening of counterfeit drugs of macrolide antibiotics. Journal of pharmaceutical and biomedical analysis, 40(1), 68-74.

Zhang, X., Xiao, K., & Tehranipoor, M. (2012). Path-delay fingerprinting for identification of recovered ICs. In Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012 IEEE International Symposium on (pp. 13-18). IEEE.

Naktuinbouw (Netherlands Inspection Service for Horticulture) 2015. http://www.naktuinbouw.nl/en/service/diagnostics. Last accessed 30 October 2015.

IEEE (2012) http://spectrum.ieee.org/semiconductors/devices/plant-dna-vs-counterfeit-chips. Last accessed 30 October 2015.

(TS 2015). Transport Security http://www.transportsecurity.com/covert-tracking-technolgy.html. Last accessed 30 October 2015.

World Health Organization (WHO) (2015). Anti-counterfeit Technologies for the Protection of Medicines. http://www.who.int/impact/events/IMPACT-ACTechnologiesv3LIS.pdf. Last accessed 30 October 2015.

Chaudhry, P. E., Zimmerman, A., Peters, J. R., & Cordell, V. V. (2009). Preserving intellectual property rights: Managerial insight into the escalating counterfeit market quandary. Business Horizons, 52(1), 57-66.

Mike Bohlman, Chair of ISO/TC 104, ISO Focus (2005). Freight containers Container security seals. www.**iso**.org. Last accessed 30 October 2015.

Ho Sung Lee; Hyo Chan Bang, "Detecting counterfeit products using supply chain event mining," *Advanced Communication Technology (ICACT), 2013 15th International Conference on* , vol., no., pp.744,748, 27-30 Jan. 2013.

WCO IPM Connected http://www.wcoipm.org/ipm-connected. Last accessed 30 October 2015.

Wired 2015. http://www.wired.com/insights/2015/02/illegal-immoral-and-here-to-stay-counterfeiting-and-the-3d-printing-revolution/. Last accessed 30 October 2015.

Gartner Predicts 2014: 3D Printing at the Inflection Point. http://www.gartner.com/doc/2631234. Last accessed 30 October 2015..

Dr Rajiv Dhar, Director, Indian Institute of Packaging for Confederation of India Industry - August 2009. Anti-Counterfeit Packaging Technologies. http://www.bilcaretech.com/pdf/whitepaper/CII_Anti_Counterfeit_Pkg_Technologies_Report_by_Dr_Dhar_Final_17Aug09.pdf. Last accessed 30 October 2015.

eBay (2015). http://pages.ebay.co.uk/safetycentre/counterfeits.html. Last accessed 30 October 2015.

BASCAP (2015). Roles and responsibilities of intermediaries: fighting counterfeiting and piracy in the supply chain.

http://www.iccwbo.org/Data/Documents/Bascap/International-engagement-and-advocacy/2015-Roles-and-Responsibilities-of-Intermediaries/. Last accessed 20 August 2015.

ISO (2012). ISO 12931:2012. Performance criteria for authentication solutions used to combat counterfeiting of material goods

BASCAP (2007). Global Survey on Counterfeiting & Piracy Survey findings report. http://www.iccwbo.org/Data/Documents/Bascap/Business-Perception/Business-Perception-Full-Report/. Last accessed 20 August 2015.

Zhang (2008). Metal-enhanced fluorescence from paper substrates: Modified spectral properties of dyes for potential high-throughput surface analysis and assays and as an anti-counterfeiting technology.

O'Connor, M. C. 2009. "Bloomingdale's Tests from Item-Level RFID," RFID Journal. http://www.rfidjournal.com/articles/view?5160,

SICPA (2015) SICPATRACE http://www.sicpa.com/government-security-solutions/sicpatrace. Last accessed 30 October 2015.

Hargreaves, M. D., Page, K., Munshi, T., Tomsett, R., Lynch, G., & Edwards, H. G. (2008). Analysis of seized drugs using portable Raman spectroscopy in an airport environment—a proof of principle study. Journal of Raman Spectroscopy, 39(7), 873-880.

Ortiz (2012). Rafael S. Ortiz, Kristiane C. Mariotti, Nicolas V. Schwab, Guilherme P. Sabin, Werickson F.C. Rocha, Eustáquio V.R. de Castro, Renata P. Limberger, Paulo Mayorga, Maria Izabel M.S. Bueno, Wanderson Romão, Fingerprinting of sildenafil citrate and tadalafil tablets in pharmaceutical formulations via X-ray fluorescence (XRF) spectrometry, Journal of Pharmaceutical and Biomedical Analysis, Volume 58, 25 January 2012, Pages 7-11, ISSN 0731-7085.

Wang (2009), Y. Wang, *Design of an anti-counterfeit system based on SMS*, IEEE International Conference on Granular Computing(GRC'09), Nanchang, China, pp.572-575, August 2009.

Yan and Huang (2008), B. Yan and G. W. Huang, *Application of RFID and Internet of Things in monitoring and anti-counterfeit for products*, International Seminar on Business and Information Management (ISBIM08), Wuhan, China, pp.392-395, December 2008

Lei et al. (2005), Pouwan Lei; Claret-Tournier, F.; Chatwin, C.; Young, R., "A secure mobile track and trace system for anti-counterfeit," e-Technology, e-Commerce and e-Service, 2005. EEE '05. Proceedings. The 2005 IEEE International Conference on , vol., no., pp.686,689, 29 March-1 April 2005

Eldefrawy et al. (2012),. Eldefrawy, M.H.; Khan, M.K., "Detecting counterfeit-money using RFID-enabled mobile devices," Internet Technology And Secured Transactions, 2012 International Conferece For , vol., no., pp.74,79, 10-12 Dec. 2012

Babu et al. (2010), Babu, H.U.; Stork, W.; Rauhe, H., "Anti-counterfeit using reflective micro structures - Based on random positioning of microstructures," Advances in Optoelectronics and Micro/Nano-Optics (AOM), 2010 OSA-IEEE-COS , vol., no., pp.,, 3-6 Dec. 2010.

Banks, J.,Hanny,D.,Pachano,M.A.,Thompson,L.G.,2007. RFIDApplied. JohnWiley & Sons,Inc.

Reischach et al. (2007), Graf von Reischach, F., Michahelles, F., Fleisch, E., Anti-counterfeit 2.0 - A Consumer-Driven Approach towards Product Authentication, Ubicomp 2007, Innsbruck, 2007.

Zheng and Xuandong (2007), Sheng Cao Zheng, Chen Xuandong Sun, Anti-Counterfeit Authentication System of Printed Information Based on A Logic Signing

Technique, Proceedings of the International Conference on Intelligent Systems and Knowledge Engineering (ISKE 2007)

Chen at al. (2005), Yuqun Chen, M. Kivanc¸ Mihc¸ak, and Darko Kirovski, Certifying Authenticity via Fiber-Infused Paper, ACM SIGecom Exchanges Homepage archive Volume 5 Issue 3, April 2005.

Rytter, W. (2000). Compressed and fully compressed pattern matching in one and two dimensions. Proceedings of the IEEE, 88(11), 1769-1778.

Warasart and Kuacharoen (2012), Maykin Warasart and Pramote Kuacharoen, Paper-based Document Authentication using Digital Signature and QR Code, 2012 4TH International Conference on Computer Engineering and Technology (ICCET 2012)

Cole and Ranasinghe (2008), Peter H. Cole · Damith C. Ranasinghe, Networked RFID Systems and Lightweight Cryptography - Raising Barriers to Product Counterfeiting, Springer 2008.

(EC 2011). Consumer Empowerment in the EU, COMMISSION STAFF WORKING PAPER, 2011. SEC(2011) 469 final http://ec.europa.eu/consumers/archive/overview/cons_policy/doc/EN_99.pdf. Last accessed 30 October 2015.

von Reischach, F., Michahelles, F., & Fleisch, E. (2007). Anti-counterfeit 2.0-A Consumer-Driven Approach towards Product Authentication. In *Late Breaking Results at the 9th International Conference on Ubiquitous Computing (UbiComp 2007), Austria*.

Sarac, A., Absi,N., Dauzere-Peres, S.,2008b. A simulation approach to evaluate the impact of introducing RFID technologies in a three-level supply chain. In: Proceedings of the 40th Conference on Winter Simulation, pp. 2741–2749. ISO (2015). ISO Strategic Plan (2011-2015). http://www.iso.org/iso/iso_strategic_plan_2011-2015.pdf. Last accessed 30 October 2015.

GROW (2015). Traceability across the Value Chain New anti-counterfeiting methods http://ec.europa.eu/growth/industry/innovation/business-innovation-observatory/files/case-studies/41-tvc-new-anti-counterfeiting-methods_en.pdf#page=3&zoom=auto,-162,676. 2015. Last accessed 30 October 2015.

Corbellini, S., Ferraris, F., & Parvis, M. (2006). A cryptographic system for brand authentication and material traceability in the textile industry. In *Instrumentation and Measurement Technology Conference, 2006. IMTC 2006. Proceedings of the IEEE* (pp. 1331-1335). IEEE.

Wang, Y. (2009). Design of an anti-counterfeit system based on SMS. In *Granular Computing, 2009, GRC'09. IEEE International Conference on* (pp. 572-575). IEEE.

Wang, J., & Yagi, Y. (2008). Integrating color and shape-texture features for adaptive real-time object tracking. IEEE Transactions on Image Processing, 17(2), 235-240.

Liu, V., Caelli, W., Foo, E., & Russell, S. (2004). Visually sealed and digitally signed documents. In *Proceedings of the 27th Australasian conference on Computer science-Volume 26* (pp. 287-294). Australian Computer Society, Inc.

Smart Devices by Adrian Burden at BilcareTechnologies http://www.bilcaretech.com/pdf/whitepaper/Technology-has-a-habit-of-converging.pdf. Last accessed August 2015.

PC World. NEC smartphone tech can spot counterfeit goods http://www.pcworld.idg.com.au/article/559250/nec-smartphone-tech-can-spot-counterfeit-goods/. Last accessed 30 October 2015..

SECRF (2015). http://www.securerf.com/. Last accessed 30 October 2015.

FINNCODE (2015). http://www.finncode.com/?page_id=50. Last accessed 30 October 2015.

Cobb, W.E.; Laspe, E.D.; Baldwin, R.O.; Temple, Michael A.; Kim, Y.C.,(2012), Intrinsic Physical-Layer Authentication of Integrated Circuits *IEEE Transactions on Information Forensics and Security,* vol.7, no.1, pp.14,24, Feb. 2012.

JRC (2012). RFID Tags Privacy Threats and Countermeasures. JR 78156 https://ec.europa.eu/jrc/sites/default/files/jrc78156_report_rfid_en.pdf. Last accessed 30 October 2015.

Williams, M.D.; Temple, Michael A.; Reising, D.R., "Augmenting Bit-Level Network Security Using Physical Layer RF-DNA Fingerprinting," *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE* , vol., no., pp.1,6, 6-10 Dec. 2010.

Telecom Digest (2014). Booming Fake Phone Market in Nigeria http://www.ittelecomdigest.com/news/security/item/55-booming-fake-phone-market-in-nigeria. Last accessed 30 October 2015.

NOKOMIS (2014) http://www.nokomisinc.com/. Last accessed 30 October 2015.

World Health Organization - Anticounterfeit technologies for the protection of medicines http://www.who.int/impact/events/IMPACT-ACTechnologiesv3LIS.pdf. Last accessed 30 October 2015.

A.1. Annex 1

Table 3 Evaluation for Fast Moving Consumers Goods

Fast moving Consumer Goods	**Technical simplicity**	**Field Identification**	**Accuracy**	**Impact to the good**	**Economic efficiency**	**Extendibility**	**Adaptability to organizations and existing processes**	**Market support**	**Level of Training**	**Technical maturity**
Authentication based on electromagnetic spectrum emissions										
Visual inspection with no augmentation	5	4	4	4	4	4	5	4	3	4
Augmented Visual inspection	4	4	5	4	4	4	4	4	3	4
Chemical reaction for visual inspection	3	3	4	2	3	3	4	4	4	4
Statistical analysis of images of the good (object recognition)	3	4	3	4	4	3	3	3	3	3
Visual Identifiers inserted in the good	4	4	4	3	3	4	4	4	4	4
Analysis of Radio Frequency emissions										
Radio Frequency Identifier	4	4	4	3	4	4	4	4	4	4
Unintentional Radio Frequency emissions	0	0	0	0	0	0	0	0	0	0
Radio Frequency Emission while transmitting	0	0	0	0	0	0	0	0	0	0
Physical Unclonable Functions (PUF)	0	0	0	0	0	0	0	0	0	0
Induced emissions										
Nuclear magnetic resonance spectroscopy	0	0	0	0	0	0	0	0	0	0
FTIR	0	0	0	0	0	0	0	0	0	0
Near-infrared spectroscopy (NIR)	0	0	0	0	0	0	0	0	0	0
Scanning Electron Microscopy (SEM)	0	0	0	0	0	0	0	0	0	0
Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)	0	0	0	0	0	0	0	0	0	0
X-Ray Inspection	0	0	0	0	0	0	0	0	0	0
X-ray fluorescence	0	0	0	0	0	0	0	0	0	0
Energy-dispersive X-ray spectroscopy	0	0	0	0	0	0	0	0	0	0
Authentication based on artefacts generated internally by the good										
Statistical analysis of images produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of audio samples produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of artefacts generated internally by the good	0	0	0	0	0	0	0	0	0	0
Electrical Inspection	0	0	0	0	0	0	0	0	0	0
Chemical Inspection	1	1	1	1	1	1	1	1	1	1
Authentication based on Weight and Structural Tests										
Thermogravimetric Analysis (TGA)	2	2	4	2	3	3	3	3	3	3
Path Delay	0	0	0	0	0	0	0	0	0	0
Authentication based on DNA	3	2	5	3	3	3	3	3	2	3
Authentication based on Acoustics tests	3	2	3	3	2	2	3	2	2	2
Track and trace technologies										
Numeric Identifier/ One dimension-Bar Code	5	5	4	4	4	4	4	5	5	5
QR code and other two dimensional bar codes	5	5	4	4	4	4	4	5	5	5
Other overt technologies	4	4	5	4	4	5	5	4	4	4
Other Covert technologies	4	4	5	4	4	5	5	4	4	4
Radio Frequency Identifier	5	5	5	4	3	4	4	4	4	5
Container tracking, packaging and sealing										
Container tracking	5	4	4	5	4	5	4	4	4	5
Container seals	5	4	4	5	4	5	5	5	4	5
Packaging	5	4	4	5	4	4	4	5	4	5
New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things										
Techniques for fight against counterfeiting in E-Commerce	4	3	3	5	4	4	4	4	4	4
Application of Internet of Things (IoT) to fight against counterfeiting	3	3	3	3	3	4	4	3	3	3
Correlation of data from difference elements/sources	4	3	4	4	3	4	3	4	3	4
Organizational and processes aspects and techniques										
Due Diligence and Supply Chain Management Responsibility	4	4	4	4	4	5	4	4	4	4
Informing consumers/Awareness	4	5	4	5	4	4	4	4	4	4
Harmonization of customs procedure	4	4	4	4	4	4	4	4	4	5

Table 4 Evaluation for Textiles

TEXTILES	Technical simplicity	Field Identification	Accuracy	Impact to the good	Economic efficiency	Extendibility	Adaptability to organizations and existing processes	Market support	Level of Training	Technical maturity
Authentication based on electromagnetic spectrum emissions										
Visual inspection with no augmentation	5	5	4	5	5	5	5	4	3	5
Augmented Visual inspection	4	4	5	5	4	5	4	4	4	4
Chemical reaction for visual inspection	3	3	5	2	3	3	4	3	3	4
Statistical analysis of images of the good (object recognition)	3	4	3	4	4	4	3	3	4	3
Visual Identifiers inserted in the good	4	4	4	3	3	4	4	4	4	4
Analysis of Radio Frequency emissions										
Radio Frequency Identifier	4	4	4	3	4	4	4	4	4	4
Unintentional Radio Frequency emissions	0	0	0	0	0	0	0	0	0	0
Radio Frequency Emission while transmitting	0	0	0	0	0	0	0	0	0	0
Physical Unclonable Functions (PUF)	0	0	0	0	0	0	0	0	0	0
Induced emissions										
Nuclear magnetic resonance spectroscopy	2	2	4	3	3	3	3	3	2	3
FTIR	2	2	4	3	3	3	3	3	2	3
Near-infrared spectroscopy (NIR)	2	2	4	3	3	3	3	3	2	3
Scanning Electron Microscopy (SEM)	2	2	4	3	3	3	3	3	2	3
Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)	2	2	4	3	3	3	3	3	2	3
X-Ray Inspection	2	2	4	3	3	3	3	3	2	3
X-ray fluorescence	2	2	4	3	3	3	3	3	2	3
Energy-dispersive X-ray spectroscopy	2	2	4	3	3	3	3	3	2	3
Authentication based on artefacts generated internally by the good										
Statistical analysis of images produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of audio samples produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of artefacts generated internally by the good	0	0	0	0	0	0	0	0	0	0
Electrical Inspection	0	0	0	0	0	0	0	0	0	0
Chemical Inspection	1	1	1	1	1	1	1	1	1	1
Authentication based on Weight and Structural Tests										
Thermogravimetric Analysis (TGA)	2	2	4	2	3	3	3	3	3	3
Path Delay	0	0	0	0	0	0	0	0	0	0
Authentication based on DNA	3	2	5	4	3	3	3	3	3	3
Authentication based on Acoustics tests	3	2	5	4	3	3	3	3	3	3
Track and trace technologies										
Numeric Identifier/ One dimension-Bar Code	5	5	4	4	4	4	4	5	5	5
QR code and other two dimensional bar codes	5	5	4	4	4	4	4	5	5	5
Other overt technologies	4	4	5	4	4	5	5	4	4	4
Other Covert technologies	4	4	5	4	4	5	5	4	4	4
Radio Frequency Identifier	5	5	5	4	3	4	4	4	4	5
Container tracking, packaging and sealing										
Container tracking	5	3	3	5	4	5	3	4	4	3
Container seals	5	4	3	5	4	5	5	5	4	5
Packaging	5	4	3	5	3	4	4	5	4	5
New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things										
Techniques for fight against counterfeiting in E-Commerce	3	3	3	5	4	4	4	3	3	4
Application of Internet of Things (IoT) to fight against counterfeiting	3	3	3	3	3	4	4	3	3	3
Correlation of data from difference elements/sources	3	3	4	4	3	4	3	3	2	3
Organizational and processes aspects and techniques										
Due Diligence and Supply Chain Management Responsibility	4	3	3	4	4	5	4	4	3	3
Informing consumers/Awareness	4	5	3	5	4	4	4	4	3	4
Harmonization of customs procedure	4	4	4	4	4	4	3	4	3	3

Table 5 Evaluation for Luxury Goods

Luxury Goods	Technical simplicity	Field Identification	Accuracy	Impact to the good	Economic efficiency	Extendibility	Adaptability to organizations and existing processes	Market support	Level of Training	Technical maturity
Authentication based on electromagnetic spectrum emissions										
Visual inspection with no augmentation	5	5	4	5	5	5	5	4	5	5
Augmented Visual inspection	4	4	5	5	4	5	4	4	4	4
Chemical reaction for visual inspection	3	3	5	1	3	3	4	3	3	4
Statistical analysis of images of the good (object recognition)	3	4	3	4	4	4	3	3	4	3
Visual Identifiers inserted in the good	4	4	4	2	4	4	4	3	4	4
Analysis of Radio Frequency emissions										
Radio Frequency Identifier	4	4	4	3	5	4	4	4	4	4
Unintentional Radio Frequency emissions	0	0	0	0	0	0	0	0	0	0
Radio Frequency Emission while transmitting	0	0	0	0	0	0	0	0	0	0
Physical Unclonable Functions (PUF)	0	0	0	0	0	0	0	0	0	0
Induced emissions										
Nuclear magnetic resonance spectroscopy	2	2	4	3	3	3	3	3	2	3
FTIR	2	2	4	3	3	3	3	3	2	3
Near-infrared spectroscopy (NIR)	2	2	4	3	3	3	3	3	2	3
Scanning Electron Microscopy (SEM)	2	2	4	3	3	3	3	3	2	3
Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)	2	2	4	3	3	3	3	3	2	3
X-Ray Inspection	2	2	4	3	3	3	3	3	2	3
X-ray fluorescence	2	2	4	3	3	3	3	3	2	3
Energy-dispersive X-ray spectroscopy	2	2	4	3	3	3	3	3	2	3
Authentication based on artefacts generated internally by the good										
Statistical analysis of images produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of audio samples produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of artefacts generated internally by the good	0	0	0	0	0	0	0	0	0	1
Electrical Inspection	0	0	0	0	0	0	0	0	0	0
Chemical Inspection	1	1	1	1	1	1	1	1	1	1
Authentication based on Weight and Structural Tests										
Thermogravimetric Analysis (TGA)	2	2	4	2	3	3	3	3	3	3
Path Delay	0	0	0	0	0	0	0	0	0	0
Authentication based on DNA	3	2	5	4	3	3	3	3	3	3
Authentication based on Acoustics tests	3	2	5	4	3	3	3	3	3	3
Track and trace technologies										
Numeric Identifier/ One dimension-Bar Code	5	5	4	4	4	4	4	5	5	5
QR code and other two dimensional bar codes	5	5	4	4	4	4	4	5	5	5
Other overt technologies	4	4	5	4	4	5	5	4	4	4
Other Covert technologies	4	4	5	4	4	5	5	4	4	4
Radio Frequency Identifier	5	5	5	4	3	4	4	4	4	5
Container tracking, packaging and sealing										
Container tracking	5	3	3	5	4	5	3	4	4	3
Container seals	5	4	3	5	4	5	5	5	4	5
Packaging	5	4	3	5	3	4	4	5	4	5
New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things										
Techniques for fight against counterfeiting in E-Commerce	3	3	3	5	4	4	4	3	3	4
Application of Internet of Things (IoT) to fight against counterfeiting	3	3	3	3	3	4	4	3	3	3
Correlation of data from difference elements/sources	3	3	4	4	3	4	3	3	2	3
Organizational and processes aspects and techniques										
Due Diligence and Supply Chain Management Responsibility	4	3	3	4	4	5	4	4	3	3
Informing consumers/Awareness	4	5	3	5	4	4	4	4	3	4
Harmonization of customs procedure	4	4	4	4	4	4	3	4	3	3

Sporting Goods	Technical simplicity	Field Identification	Accuracy	Impact to the good	Economic efficiency	Extendibility	Adaptability to organizations and existing processes	Market support	Level of Training	Technical maturity
Authentication based on electromagnetic spectrum emissions										
Visual inspection with no augmentation	5	5	4	5	5	5	5	4	4	5
Augmented Visual inspection	4	4	5	5	4	5	4	4	4	4
Chemical reaction for visual inspection	4	4	5	3	3	3	4	4	3	4
Statistical analysis of images of the good (object recognition)	3	4	4	4	4	4	3	3	4	3
Visual Identifiers inserted in the good	4	4	4	2	4	4	4	3	4	4
Analysis of Radio Frequency emissions										
Radio Frequency Identifier	4	4	4	3	5	4	4	4	4	4
Unintentional Radio Frequency emissions	0	0	0	0	0	0	0	0	0	0
Radio Frequency Emission while transmitting	0	0	0	0	0	0	0	0	0	0
Physical Unclonable Functions (PUF)	0	0	0	0	0	0	0	0	0	0
Induced emissions										
Nuclear magnetic resonance spectroscopy	2	2	4	3	3	3	3	3	2	3
FTIR	2	2	4	3	3	3	3	3	2	3
Near-infrared spectroscopy (NIR)	2	2	4	3	3	3	3	3	2	3
Scanning Electron Microscopy (SEM)	2	2	4	3	3	3	3	3	2	3
Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)	2	2	4	3	3	3	3	3	2	3
X-Ray Inspection	2	2	4	3	3	3	3	3	2	3
X-ray fluorescence	2	2	4	3	3	3	3	3	2	3
Energy-dispersive X-ray spectroscopy	2	2	4	3	3	3	3	3	2	3
Authentication based on artefacts generated internally by the good										
Statistical analysis of images produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of audio samples produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of artefacts generated internally by the good	0	0	0	0	0	0	0	0	0	1
Electrical Inspection	0	0	0	0	0	0	0	0	0	0
Chemical Inspection	1	1	1	1	1	1	1	1	1	1
Authentication based on Weight and Structural Tests										
Thermogravimetric Analysis (TGA)	2	2	4	2	3	3	3	3	3	3
Path Delay	0	0	0	0	0	0	0	0	0	0
Authentication based on DNA	3	2	5	4	3	3	3	3	3	3
Authentication based on Acoustics tests	3	2	5	4	3	3	3	3	3	3
Track and trace technologies										
Numeric Identifier/ One dimension-Bar Code	5	5	4	4	4	4	4	5	5	5
QR code and other two dimensional bar codes	5	5	4	4	4	4	4	5	5	5
Other overt technologies	4	4	5	4	4	5	5	4	4	4
Other Covert technologies	4	4	5	4	4	5	5	4	4	4
Radio Frequency Identifier	5	5	5	4	3	4	4	4	4	5
Container tracking, packaging and sealing										
Container tracking	5	3	3	5	4	5	3	4	4	3
Container seals	5	4	3	5	4	5	5	5	4	5
Packaging	5	4	3	5	3	4	4	5	4	5
New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things										
Techniques for fight against counterfeiting in E-Commerce	3	3	3	5	4	4	4	3	3	4
Application of Internet of Things (IoT) to fight against counterfeiting	3	3	3	3	3	4	4	3	3	3
Correlation of data from difference elements/sources	3	3	4	4	3	4	3	3	2	3
Organizational and processes aspects and techniques										
Due Diligence and Supply Chain Management Responsibility	4	3	3	4	4	5	4	4	3	3
Informing consumers/Awareness	4	5	3	5	4	4	4	4	3	4
Harmonization of customs procedure	4	4	4	4	4	4	3	4	3	3

Table 6 Evaluation for Electronics/Semiconductors

Electronics-Semiconductors	**Technical simplicity**	**Field Identification**	**Accuracy**	**Impact to the good**	**Economic efficiency**	**Extendibility**	**Adaptability to organizations and existing processes**	**Market support**	**Level of Training**	**Technical maturity**
Authentication based on electromagnetic spectrum emissions										
Visual inspection with no augmentation	3	3	2	5	5	4	4	4	2	4
Augmented Visual inspection	3	3	3	5	4	4	4	4	4	4
Chemical reaction for visual inspection	4	3	4	2	3	3	4	3	3	3
Statistical analysis of images of the good (object recognition)	3	3	3	4	4	4	4	3	4	3
Visual Identifiers inserted in the good	3	2	3	2	2	3	2	2	2	3
Analysis of Radio Frequency emissions										
Radio Frequency Identifier	3	3	4	2	2	3	4	3	3	3
Unintentional Radio Frequency emissions	3	2	3	4	3	1	2	3	2	3
Radio Frequency Emission while transmitting	3	2	3	4	3	1	2	3	2	3
Physical Unclonable Functions (PUF)	3	4	5	4	3	3	3	4	4	4
Induced emissions										
Nuclear magnetic resonance spectroscopy	2	2	4	4	2	3	4	3	2	4
FTIR	2	2	3	4	2	3	4	3	2	4
Near-infrared spectroscopy (NIR)	2	2	2	4	2	2	4	3	2	4
Scanning Electron Microscopy (SEM)	2	1	5	2	3	3	3	3	1	4
Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)	2	1	5	2	3	3	3	3	1	4
X-Ray Inspection	3	2	4	4	3	3	3	4	1	4
X-ray fluorescence	3	2	5	4	3	3	3	4	1	4
Energy-dispersive X-ray spectroscopy	3	2	5	4	3	3	3	4	1	4
Authentication based on artefacts generated internally by the good										
Statistical analysis of images produced by the good	2	1	3	3	3	2	2	2	2	2
Statistical analysis of audio samples produced by the good	2	1	4	4	2	3	3	2	2	2
Statistical analysis of artefacts generated internally by the good	3	2	4	4	4	4	3	2	2	1
Electrical Inspection	4	3	4	4	3	4	3	4	3	4
Chemical Inspection	4	3	4	3	3	4	3	4	3	4
Authentication based on Weight and Structural Tests										
Thermogravimetric Analysis (TGA)	3	2	3	3	3	3	3	3	3	4
Path Delay	3	2	4	4	4	4	4	3	2	3
Authentication based on DNA	0	0	0	0	0	0	0	0	0	0
Authentication based on Acoustics tests (SAM)	3	2	4	4	4	4	4	4	3	4
Track and trace technologies										
Numeric Identifier/ One dimension-Bar Code	3	3	3	5	3	3	4	4	3	4
QR code and other two dimensional bar codes	3	3	3	5	3	3	4	4	3	4
Other overt technologies	4	5	4	4	4	4	4	4	4	4
Other Covert technologies	4	4	5	4	4	4	4	4	4	4
Radio Frequency Identifier	3	3	4	2	2	3	3	3	4	3
Container tracking, packaging and sealing										
Container tracking	5	3	3	5	4	5	3	4	4	3
Container seals	5	4	3	5	4	5	5	5	4	5
Packaging	5	4	3	5	3	4	4	5	4	5
New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things										
Techniques for fight against counterfeiting in E-Commerce	3	3	3	5	4	4	4	3	3	4
Application of Internet of Things (IoT) to fight against counterfeiting	3	3	3	3	3	4	4	3	3	3
Correlation of data from difference elements/sources	3	3	4	4	3	4	4	3	3	4
Organizational and processes aspects and techniques										
Due Diligence and Supply Chain Management Responsibility	4	3	4	5	4	5	4	4	3	4
Informing consumers/Awareness	3	3	2	4	3	3	4	3	3	3
Harmonization of customs procedure	4	4	4	4	4	4	3	4	3	3

Table 7 Evaluation for Smartphone/Tablets

Smartphone/Tablets	Technical simplicity	Field Identification	Accuracy	Impact to the good	Economic efficiency	Extendibility	Adaptability to organizations and existing processes	Market support	Level of Training	Technical maturity
Authentication based on electromagnetic spectrum emissions										
Visual inspection with no augmentation	5	5	4	5	5	5	5	4	5	5
Augmented Visual inspection	4	4	5	5	4	5	4	4	4	4
Chemical reaction for visual inspection	3	3	3	2	3	3	4	3	3	3
Statistical analysis of images of the good (object recognition)	3	3	3	4	4	4	4	3	4	3
Visual Identifiers inserted in the good	3	4	4	3	3	4	3	3	4	4
Analysis of Radio Frequency emissions										
Radio Frequency Identifier	4	4	4	4	3	4	4	4	4	4
Unintentional Radio Frequency emissions	3	2	3	4	3	1	2	3	2	3
Radio Frequency Emission while transmitting	4	4	4	4	4	3	4	3	3	3
Physical Unclonable Functions (PUF)	3	3	5	3	3	3	3	4	3	4
Induced emissions										
Nuclear magnetic resonance spectroscopy	2	2	4	3	3	3	3	3	2	3
FTIR	2	2	4	3	3	3	3	3	2	3
Near-infrared spectroscopy (NIR)	2	2	4	3	3	3	3	3	2	3
Scanning Electron Microscopy (SEM)	2	2	4	3	3	3	3	3	2	3
Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)	2	2	4	3	3	3	3	3	2	3
X-Ray Inspection	2	2	4	3	3	3	3	3	2	3
X-ray fluorescence	2	2	4	3	3	3	3	3	2	3
Energy-dispersive X-ray spectroscopy	2	2	4	3	3	3	3	3	2	3
Authentication based on artefacts generated internally by the good										
Statistical analysis of images produced by the good	4	4	4	4	4	3	3	3	4	3
Statistical analysis of audio samples produced by the good	4	4	4	4	4	3	3	3	4	3
Statistical analysis of artefacts generated internally by the good	4	4	4	4	4	3	3	3	4	3
Electrical Inspection	3	2	3	3	3	4	4	4	3	4
Chemical Inspection	3	3	3	3	3	4	4	4	3	4
Authentication based on Weight and Structural Tests										
Thermogravimetric Analysis (TGA)	3	2	3	3	3	3	3	3	3	4
Path Delay	3	2	4	4	4	4	4	3	2	3
Authentication based on DNA	0	0	0	0	0	0	0	0	0	0
Authentication based on Acoustics tests (SAM)	3	2	4	3	3	4	4	3	3	3
Track and trace technologies										
Numeric Identifier/ One dimension-Bar Code	5	5	4	4	4	4	4	5	5	5
QR code and other two dimensional bar codes	5	5	4	4	4	4	4	5	5	5
Other overt technologies	4	4	5	4	4	5	5	4	4	4
Other Covert technologies	4	4	5	4	4	5	5	4	4	4
Radio Frequency Identifier	5	5	5	4	3	4	4	4	4	5
Container tracking, packaging and sealing										
Container tracking	5	3	3	5	4	5	3	4	4	3
Container seals	5	4	3	5	4	5	5	5	4	5
Packaging	5	4	3	5	3	4	4	5	4	5
New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things										
Techniques for fight against counterfeiting in E-Commerce	3	3	3	5	4	4	4	3	3	4
Application of Internet of Things (IoT) to fight against counterfeiting	3	3	3	3	3	4	4	3	3	3
Correlation of data from difference elements/sources	3	3	4	4	3	4	3	3	2	3
Organizational and processes aspects and techniques										
Due Diligence and Supply Chain Management Responsibility	4	3	3	4	4	5	4	4	3	3
Informing consumers/Awareness	4	5	3	5	4	4	4	4	3	4
Harmonization of customs procedure	4	4	4	4	4	4	3	4	3	3

Table 8 Evaluation for Food

Food	Technical simplicity	Field Identification	Accuracy	Impact to the good	Economic efficiency	Extendibility	Adaptability to organizations and existing processes	Market support	Level of Training	Technical maturity
Authentication based on electromagnetic spectrum emissions										
Visual inspection with no augmentation	5	4	4	4	4	4	5	4	3	4
Augmented Visual inspection	4	4	5	4	4	4	4	4	3	4
Chemical reaction for visual inspection	3	3	4	2	3	3	4	4	4	4
Statistical analysis of images of the good (object recognition)	3	4	3	4	4	3	3	3	3	3
Visual Identifiers inserted in the good	4	4	4	3	3	4	4	4	4	4
Analysis of Radio Frequency emissions										
Radio Frequency Identifier	4	4	4	3	4	4	4	4	4	4
Unintentional Radio Frequency emissions	0	0	0	0	0	0	0	0	0	0
Radio Frequency Emission while transmitting	0	0	0	0	0	0	0	0	0	0
Physical Unclonable Functions (PUF)	0	0	0	0	0	0	0	0	0	0
Induced emissions										
Nuclear magnetic resonance spectroscopy	0	0	0	0	0	0	0	0	0	0
FTIR	0	0	0	0	0	0	0	0	0	0
Near-infrared spectroscopy (NIR)	0	0	0	0	0	0	0	0	0	0
Scanning Electron Microscopy (SEM)	0	0	0	0	0	0	0	0	0	0
Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)	0	0	0	0	0	0	0	0	0	0
X-Ray Inspection	0	0	0	0	0	0	0	0	0	0
X-ray fluorescence	0	0	0	0	0	0	0	0	0	0
Energy-dispersive X-ray spectroscopy	0	0	0	0	0	0	0	0	0	0
Authentication based on artefacts generated internally by the good										
Statistical analysis of images produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of audio samples produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of artefacts generated internally by the good	0	0	0	0	0	0	0	0	0	0
Electrical Inspection	0	0	0	0	0	0	0	0	0	0
Chemical Inspection	1	1	1	1	1	1	1	1	1	1
Authentication based on Weight and Structural Tests										
Thermogravimetric Analysis (TGA)	2	2	4	2	3	3	3	3	3	3
Path Delay	0	0	0	0	0	0	0	0	0	0
Authentication based on DNA	3	2	5	3	3	3	3	3	2	3
Authentication based on Acoustics tests	3	2	3	3	2	2	3	2	2	2
Track and trace technologies										
Numeric Identifier/ One dimension-Bar Code	5	5	4	4	4	4	4	5	5	5
QR code and other two dimensional bar codes	5	5	4	4	4	4	4	5	5	5
Other overt technologies	4	4	5	4	4	5	5	4	4	4
Other Covert technologies	4	4	5	4	4	5	5	4	4	4
Radio Frequency Identifier	5	5	5	4	3	4	4	4	4	5
Container tracking, packaging and sealing										
Container tracking	5	4	4	5	4	5	4	4	4	5
Container seals	5	4	4	5	4	5	5	5	4	5
Packaging	5	4	4	5	4	4	4	5	4	5
New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things										
Techniques for fight against counterfeiting in E-Commerce	4	3	3	5	4	4	4	4	4	4
Application of Internet of Things (IoT) to fight against counterfeiting	3	3	3	3	3	4	4	3	3	3
Correlation of data from difference elements/sources	4	3	4	4	3	4	3	4	3	4
Organizational and processes aspects and techniques										
Due Diligence and Supply Chain Management Responsibility	4	4	4	4	4	5	4	4	4	4
Informing consumers/Awareness	4	5	4	5	4	4	4	4	4	4
Harmonization of customs procedure	4	4	4	4	4	4	4	4	4	5

Table 9 Evaluation for Medicines

Medicines	Technical simplicity	Field Identification	Accuracy	Impact to the good	Economic efficiency	Extendibility	Adaptability to organizations and existing processes	Market support	Level of Training	Technical maturity
Authentication based on electromagnetic spectrum emissions										
Visual inspection with no augmentation	5	4	4	4	4	4	5	4	3	4
Augmented Visual inspection	4	4	5	4	4	4	4	4	3	4
Chemical reaction for visual inspection	3	3	4	2	3	3	4	4	4	4
Statistical analysis of images of the good (object recognition)	3	4	3	4	4	3	3	3	3	3
Visual Identifiers inserted in the good	4	4	4	3	3	4	4	4	4	4
Analysis of Radio Frequency emissions										
Radio Frequency Identifier	4	4	4	4	4	4	4	4	4	4
Unintentional Radio Frequency emissions	0	0	0	0	0	0	0	0	0	0
Radio Frequency Emission while transmitting	0	0	0	0	0	0	0	0	0	0
Physical Unclonable Functions (PUF)	0	0	0	0	0	0	0	0	0	0
Induced emissions										
Nuclear magnetic resonance spectroscopy	3	3	5	4	3	3	3	4	3	5
FTIR	3	4	5	4	3	3	3	4	4	5
Near-infrared spectroscopy (NIR)	4	3	4	4	3	3	3	4	4	5
Scanning Electron Microscopy (SEM)	3	2	4	4	3	3	3	4	4	4
Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)	3	2	4	4	3	3	3	4	4	4
X-Ray Inspection	3	2	3	3	3	3	3	4	4	4
X-ray fluorescence	3	2	3	3	3	3	3	4	4	4
Energy-dispersive X-ray spectroscopy	3	2	3	3	3	3	3	4	4	4
Authentication based on artefacts generated internally by the good										
Statistical analysis of images produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of audio samples produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of artefacts generated internally by the good	0	0	0	0	0	0	0	0	0	0
Electrical Inspection	0	0	0	0	0	0	0	0	0	0
Chemical Inspection	3	4	4	3	3	3	4	4	3	4
Authentication based on Weight and Structural Tests										
Thermogravimetric Analysis (TGA)	3	2	3	2	3	3	3	3	3	3
Path Delay	0	0	0	0	0	0	0	0	0	0
Authentication based on DNA	3	2	3	3	3	3	3	3	2	3
Authentication based on Acoustics tests	0	0	0	0	0	0	0	0	0	0
Track and trace technologies										
Numeric Identifier/ One dimension-Bar Code	5	5	4	4	4	4	4	5	5	5
QR code and other two dimensional bar codes	5	5	4	4	4	4	4	5	5	5
Other overt technologies	4	4	5	4	4	5	5	4	4	4
Other Covert technologies	4	4	5	4	4	5	5	4	4	4
Radio Frequency Identifier	5	5	5	4	3	4	4	4	4	5
Container tracking, packaging and sealing										
Container tracking	4	4	4	5	4	5	4	4	4	5
Container seals	4	4	4	5	4	5	5	5	4	5
Packaging	5	4	4	5	4	4	4	5	4	5
New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things										
Techniques for fight against counterfeiting in E-Commerce	4	3	3	5	4	4	4	4	4	4
Application of Internet of Things (IoT) to fight against counterfeiting	3	3	3	3	3	4	4	3	3	3
Correlation of data from difference elements/sources	3	3	3	3	3	4	3	4	3	4
Organizational and processes aspects and techniques										
Due Diligence and Supply Chain Management Responsibility	4	4	4	4	4	5	4	4	4	4
Informing consumers/Awareness	4	5	4	5	4	4	4	4	4	4
Harmonization of customs procedure	4	4	4	4	4	4	4	4	4	5

Table 10 Evaluation for Medical Devices

Medical Devices	Technical simplicity	Field Identification	Accuracy	Impact to the good	Economic efficiency	Extendibility	Adaptability to organizations and existing processes	Market support	Level of Training	Technical maturity
Authentication based on electromagnetic spectrum emissions										
Visual inspection with no augmentation	5	5	4	5	5	5	5	4	5	5
Augmented Visual inspection	4	4	5	5	4	5	4	4	4	4
Chemical reaction for visual inspection	3	3	3	2	3	3	4	3	3	3
Statistical analysis of images of the good (object recognition)	3	3	3	4	4	4	4	3	4	3
Visual Identifiers inserted in the good	3	4	4	3	3	4	3	3	4	4
Analysis of Radio Frequency emissions										
Radio Frequency Identifier	5	5	4	3	3	4	4	4	5	5
Unintentional Radio Frequency emissions	0	0	0	0	0	0	0	0	0	0
Radio Frequency Emission while transmitting	0	0	0	0	0	0	0	0	0	0
Physical Unclonable Functions (PUF)	0	0	0	0	0	0	0	0	0	0
Induced emissions										
Nuclear magnetic resonance spectroscopy	0	0	0	0	0	0	0	0	0	0
FTIR	0	0	0	0	0	0	0	0	0	0
Near-infrared spectroscopy (NIR)	0	0	0	0	0	0	0	0	0	0
Scanning Electron Microscopy (SEM)	0	0	0	0	0	0	0	0	0	0
Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)	0	0	0	0	0	0	0	0	0	0
X-Ray Inspection	0	0	0	0	0	0	0	0	0	0
X-ray fluorescence	0	0	0	0	0	0	0	0	0	0
Energy-dispersive X-ray spectroscopy	0	0	0	0	0	0	0	0	0	0
Authentication based on artefacts generated internally by the good										
Statistical analysis of images produced by the good	3	2	3	4	4	3	3	2	2	2
Statistical analysis of audio samples produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of artefacts generated internally by the good	3	2	3	4	4	3	3	2	2	2
Electrical Inspection	4	3	4	4	3	4	3	4	3	4
Chemical Inspection	0	0	0	0	0	0	0	0	0	0
Authentication based on Weight and Structural Tests										
Thermogravimetric Analysis (TGA)	0	0	0	0	0	0	0	0	0	0
Path Delay	3	2	4	4	4	4	4	3	2	3
Authentication based on DNA	0	0	0	0	0	0	0	0	0	0
Authentication based on Acoustics tests (SAM)	3	2	4	4	4	4	4	4	3	4
Track and trace technologies										
Numeric Identifier/ One dimension-Bar Code	5	5	3	5	5	5	5	5	5	5
QR code and other two dimensional bar codes	5	5	4	4	5	5	5	5	5	5
Other overt technologies	4	5	4	4	4	4	4	4	4	4
Other Covert technologies	4	4	5	4	4	4	4	4	4	4
Radio Frequency Identifier	4	4	4	3	3	4	4	4	4	4
Container tracking, packaging and sealing										
Container tracking	5	3	3	5	4	5	3	4	4	3
Container seals	5	4	3	5	4	5	5	5	4	5
Packaging	5	4	3	5	3	4	4	5	4	5
New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things										
Techniques for fight against counterfeiting in E-Commerce	3	3	3	5	4	4	4	3	3	3
Application of Internet of Things (IoT) to fight against counterfeiting	3	3	3	3	3	3	3	3	3	3
Correlation of data from difference elements/sources	3	3	3	3	3	3	3	3	3	3
Organizational and processes aspects and techniques										
Due Diligence and Supply Chain Management Responsibility	4	3	4	4	4	5	4	4	3	4
Informing consumers/Awareness	4	4	3	5	4	3	3	3	3	3
Harmonization of customs procedure	4	4	4	4	4	4	3	4	3	3

Table 11 Evaluation for Agricultural products

Agricoltural products	Technical simplicity	Field Identification	Accuracy	Impact to the good	Economic efficiency	Extendibility	Adaptability to organizations and existing processes	Market support	Level of Training	Technical maturity
Authentication based on electromagnetic spectrum emissions										
Visual inspection with no augmentation	5	4	4	4	4	4	5	4	3	4
Augmented Visual inspection	4	4	5	4	4	4	4	4	3	4
Chemical reaction for visual inspection	3	3	4	2	3	3	4	4	4	4
Statistical analysis of images of the good (object recognition)	3	4	3	4	4	3	3	3	3	3
Visual Identifiers inserted in the good	4	4	4	3	3	4	4	4	4	4
Analysis of Radio Frequency emissions										
Radio Frequency Identifier	4	4	4	3	4	4	4	4	4	4
Unintentional Radio Frequency emissions	0	0	0	0	0	0	0	0	0	0
Radio Frequency Emission while transmitting	0	0	0	0	0	0	0	0	0	0
Physical Unclonable Functions (PUF)	0	0	0	0	0	0	0	0	0	0
Induced emissions										
Nuclear magnetic resonance spectroscopy	0	0	0	0	0	0	0	0	0	0
FTIR	0	0	0	0	0	0	0	0	0	0
Near-infrared spectroscopy (NIR)	0	0	0	0	0	0	0	0	0	0
Scanning Electron Microscopy (SEM)	0	0	0	0	0	0	0	0	0	0
Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)	0	0	0	0	0	0	0	0	0	0
X-Ray Inspection	0	0	0	0	0	0	0	0	0	0
X-ray fluorescence	0	0	0	0	0	0	0	0	0	0
Energy-dispersive X-ray spectroscopy	0	0	0	0	0	0	0	0	0	0
Authentication based on artefacts generated internally by the good										
Statistical analysis of images produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of audio samples produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of artefacts generated internally by the good	0	0	0	0	0	0	0	0	0	0
Electrical Inspection	0	0	0	0	0	0	0	0	0	0
Chemical Inspection	1	1	1	1	1	1	1	1	1	1
Authentication based on Weight and Structural Tests										
Thermogravimetric Analysis (TGA)	2	2	4	2	3	3	3	3	3	3
Path Delay	0	0	0	0	0	0	0	0	0	0
Authentication based on DNA	3	2	5	3	3	3	3	3	2	3
Authentication based on Acoustics tests	3	2	3	3	2	2	3	2	2	2
Track and trace technologies										
Numeric Identifier/ One dimension-Bar Code	5	5	4	4	4	4	4	5	5	5
QR code and other two dimensional bar codes	5	5	4	4	4	4	4	5	5	5
Other overt technologies	4	4	5	4	4	5	5	4	4	4
Other Covert technologies	4	4	5	4	4	5	5	4	4	4
Radio Frequency Identifier	5	5	5	4	3	4	4	4	4	5
Container tracking, packaging and sealing										
Container tracking	5	4	4	5	4	5	4	4	4	5
Container seals	5	4	4	5	4	5	5	5	4	5
Packaging	5	4	4	5	4	4	4	5	4	5
New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things										
Techniques for fight against counterfeiting in E-Commerce	4	3	3	5	4	4	4	4	4	4
Application of Internet of Things (IoT) to fight against counterfeiting	3	3	3	3	3	4	4	3	3	3
Correlation of data from difference elements/sources	4	3	4	4	3	4	3	4	3	4
Organizational and processes aspects and techniques										
Due Diligence and Supply Chain Management Responsibility	4	4	4	4	4	5	4	4	4	4
Informing consumers/Awareness	4	5	4	5	4	4	4	4	4	4
Harmonization of customs procedure	4	4	4	4	4	4	4	4	4	5

Table 12 Evaluation for Agrichemicals

Agrichemicals	Technical simplicity	Field Identification	Accuracy	Impact to the good	Economic efficiency	Extendibility	Adaptability to organizations and existing processes	Market support	Level of Training	Technical maturity
Authentication based on electromagnetic spectrum emissions										
Visual inspection with no augmentation	5	4	3	4	4	4	4	4	3	4
Augmented Visual inspection	4	4	3	4	4	4	4	4	3	4
Chemical reaction for visual inspection	4	4	5	3	3	3	4	4	4	4
Statistical analysis of images of the good (object recognition)	4	4	3	4	4	3	3	3	3	3
Visual Identifiers inserted in the good	0	0	0	0	0	0	0	0	0	0
Analysis of Radio Frequency emissions										
Radio Frequency Identifier	4	4	4	3	4	4	4	4	4	4
Unintentional Radio Frequency emissions	0	0	0	0	0	0	0	0	0	0
Radio Frequency Emission while transmitting	0	0	0	0	0	0	0	0	0	0
Physical Unclonable Functions (PUF)	0	0	0	0	0	0	0	0	0	0
Induced emissions										
Nuclear magnetic resonance spectroscopy	3	3	4	4	3	3	4	4	3	4
FTIR	3	3	5	4	3	4	4	4	3	4
Near-infrared spectroscopy (NIR)	0	0	0	0	0	0	0	0	0	0
Scanning Electron Microscopy (SEM)	0	0	0	0	0	0	0	0	0	0
Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)	0	0	0	0	0	0	0	0	0	0
X-Ray Inspection	0	0	0	0	0	0	0	0	0	0
X-ray fluorescence	0	0	0	0	0	0	0	0	0	0
Energy-dispersive X-ray spectroscopy	0	0	0	0	0	0	0	0	0	0
Authentication based on artefacts generated internally by the good										
Statistical analysis of images produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of audio samples produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of artefacts generated internally by the good	0	0	0	0	0	0	0	0	0	0
Electrical Inspection	0	0	0	0	0	0	0	0	0	0
Chemical Inspection	4	4	3	3	4	3	4	4	4	4
Authentication based on Weight and Structural Tests										
Thermogravimetric Analysis (TGA)	2	2	4	2	3	3	3	3	3	4
Path Delay	0	0	0	0	0	0	0	0	0	0
Authentication based on DNA	3	2	5	3	3	3	3	3	2	3
Authentication based on Acoustics tests	3	2	3	3	2	2	3	2	2	2
Track and trace technologies										
Numeric Identifier/ One dimension-Bar Code	5	5	4	4	4	4	4	5	5	5
QR code and other two dimensional bar codes	5	5	4	4	4	4	4	5	5	5
Other overt technologies	4	4	5	4	4	5	5	4	4	4
Other Covert technologies	4	4	5	4	4	5	5	4	4	4
Radio Frequency Identifier	5	5	5	4	3	4	4	4	4	5
Container tracking, packaging and sealing										
Container tracking	5	4	4	5	4	5	4	4	4	5
Container seals	5	4	4	5	4	5	5	5	4	5
Packaging	5	4	4	5	4	4	4	5	4	5
New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things										
Techniques for fight against counterfeiting in E-Commerce	0	0	0	0	0	0	0	0	0	0
Application of Internet of Things (IoT) to fight against counterfeiting	0	0	0	0	0	0	0	0	0	0
Correlation of data from difference elements/sources	0	0	0	0	0	0	0	0	0	0
Organizational and processes aspects and techniques										
Due Diligence and Supply Chain Management Responsibility	4	4	4	4	4	5	4	4	4	4
Informing consumers/Awareness	4	4	3	5	4	4	4	3	3	4
Harmonization of customs procedure	4	4	4	4	4	4	4	4	4	5

Table 13 Evaluation for Crops and Plants

Crops and Plants	Technical simplicity	Field Identification	Accuracy	Impact to the good	Economic efficiency	Extendibility	Adaptability to organizations and existing processes	Market support	Level of Training	Technical maturity
Authentication based on electromagnetic spectrum emissions										
Visual inspection with no augmentation	4	4	3	3	4	3	4	3	3	3
Augmented Visual inspection	4	4	4	4	4	4	4	3	3	3
Chemical reaction for visual inspection	3	3	3	2	3	3	3	3	3	3
Statistical analysis of images of the good (object recognition)	3	3	3	4	4	3	3	3	3	3
Visual Identifiers inserted in the good	4	4	4	3	3	4	4	4	4	4
Analysis of Radio Frequency emissions										
Radio Frequency Identifier	4	4	4	3	4	4	4	4	4	4
Unintentional Radio Frequency emissions	0	0	0	0	0	0	0	0	0	0
Radio Frequency Emission while transmitting	0	0	0	0	0	0	0	0	0	0
Physical Unclonable Functions (PUF)	0	0	0	0	0	0	0	0	0	0
Induced emissions										
Nuclear magnetic resonance spectroscopy	0	0	0	0	0	0	0	0	0	0
FTIR	0	0	0	0	0	0	0	0	0	0
Near-infrared spectroscopy (NIR)	0	0	0	0	0	0	0	0	0	0
Scanning Electron Microscopy (SEM)	0	0	0	0	0	0	0	0	0	0
Scanning electron microscopy (SEM) in combination with electron dispersive spectroscopy (EDS)	0	0	0	0	0	0	0	0	0	0
X-Ray Inspection	0	0	0	0	0	0	0	0	0	0
X-ray fluorescence	0	0	0	0	0	0	0	0	0	0
Energy-dispersive X-ray spectroscopy	0	0	0	0	0	0	0	0	0	0
Authentication based on artefacts generated internally by the good										
Statistical analysis of images produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of audio samples produced by the good	0	0	0	0	0	0	0	0	0	0
Statistical analysis of artefacts generated internally by the good	0	0	0	0	0	0	0	0	0	0
Electrical Inspection	0	0	0	0	0	0	0	0	0	0
Chemical Inspection	0	0	0	0	0	0	0	0	0	0
Authentication based on Weight and Structural Tests										
Thermogravimetric Analysis (TGA)	2	2	4	2	3	3	3	3	3	3
Path Delay	0	0	0	0	0	0	0	0	0	0
Authentication based on DNA	3	2	5	3	3	3	3	4	3	4
Authentication based on Acoustics tests	0	0	0	0	0	0	0	0	0	0
Track and trace technologies										
Numeric Identifier/ One dimension-Bar Code	5	5	4	4	4	4	4	5	5	5
QR code and other two dimensional bar codes	5	5	4	4	4	4	4	5	5	5
Other overt technologies	4	4	5	4	4	5	5	4	4	4
Other Covert technologies	4	4	5	4	4	5	5	4	4	4
Radio Frequency Identifier	5	5	5	4	3	4	4	4	4	5
Container tracking, packaging and sealing										
Container tracking	5	4	4	5	4	5	4	4	4	5
Container seals	5	4	4	5	4	5	5	5	4	5
Packaging	4	3	4	5	4	4	4	4	4	4
New Trends and technologies: Analysis of e-Commerce web sites and Internet of Things										
Techniques for fight against counterfeiting in E-Commerce	4	3	3	5	4	4	4	4	4	4
Application of Internet of Things (IoT) to fight against counterfeiting	3	3	3	3	3	4	4	3	3	3
Correlation of data from difference elements/sources	0	0	0	0	0	0	0	0	0	0
Organizational and processes aspects and techniques										
Due Diligence and Supply Chain Management Responsibility	4	4	4	4	4	5	4	4	4	4
Informing consumers/Awareness	3	3	3	3	3	3	3	3	3	3
Harmonization of customs procedure	3	3	3	3	3	3	3	3	3	3

List of abbreviations and definitions

Glossary

ACTA	Anti-Counterfeiting Trade Agreement
BASCAP	Business Action to Stop Counterfeiting and Piracy
CCP	Customs Organization Global Container Control Programme (CCP)
COAs	Certificate Of Authenticity (COAs)
COAs	Privilege Management Infrastructure (COAs)
DARPA	Defense Advanced Research Projects Agency
EDS	Electron Dispersive Spectroscopy
EPC	EPC (electronic product code).
FMCG	Fast Moving Consumer Goods
FTIR	Fourier Transform Infrared Spectroscopy
GNSS	Global Navigation Satellite Systems
GTIN	Global Trade Identification Number
GUI	Graphical User Interface
OHIM	Office for Harmonization in the Internal Market
IC	Integrated Circuits
IoT	Internet of Things (IoT)
IP	Intellectual Property
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
NFC	Near Field Communication
NIR	Near-infrared spectroscopy
PUF	Physical Unclonable Function
QR Code	Quick Response Code
PET	Privacy Enhancing Technlogy
RFID	Radio Frequency Identifier

SAM	Scanning Acoustic Microscopy
SEM	Scanning Electron Microscopy
TGA	Thermogravimetric Analysis
UHF	Ultra High Frequency
USB	Universal Serial Bus
UV	Ultra-Violet
WCO	World Customs Organization
WHO	World Health Organization

Definitions

authentication tool	set of hardware and/or software system(s) that is part of an anticounterfeiting solution and is used to control of the authentication element (From ISO 12931:2012)
covert authentication element	Authentication element which is hidden from the human senses until the use of a tool by an informed person reveals it to their senses or else allows automated interpretation of the element (From ISO 12931:2012)
counterfeit (verb)	to simulate, reproduce or modify a material good or its packaging without authorization (From ISO 12931:2012)
counterfeit good	material good imitating or copying an authentic material good (From ISO 12931:2012)
counterfeiting	Counterfeiting and piracy are terms used to describe a range of illicit activities linked to intellectual property rights (IPR) infringement. (Source OECD)
counterfeit trademark goods	goods, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such goods, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the owner of the trademark in question under the law of the country of importation (From The Agreement on Trade-Related Aspects of Intellectual Property Rights)
forensic analysis	scientific methodology for authenticating material goods by confirming an authentication element or an intrinsic attribute through the use of specialised equipment by a skilled expert with special knowledge (From ISO 12931:2012)
overt authentication element	Authentication element which is detectable and verifiable by one or more of the human senses without resource to a tool (other than everyday tools which correct imperfect human senses, such as spectacles or hearing aids) (From ISO 12931:2012)
rights holder	physical person or legal entity either holding or authorised to use one or more intellectual property rights (From ISO 12931:2012)
technique	Technique is a technology and/or a process or both, which can be used in the fight against the production and distribution of counterfeit products.

track and trace	Means of identifying every individual material good or lot(s) or batch in order to know where it has been (track) and where it is (trace) in the supply chain.

List of figures

List of tables

LB-NA-27688-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

Publications Office

doi:10.2788/97231

ISBN 978-92-79-54544-3