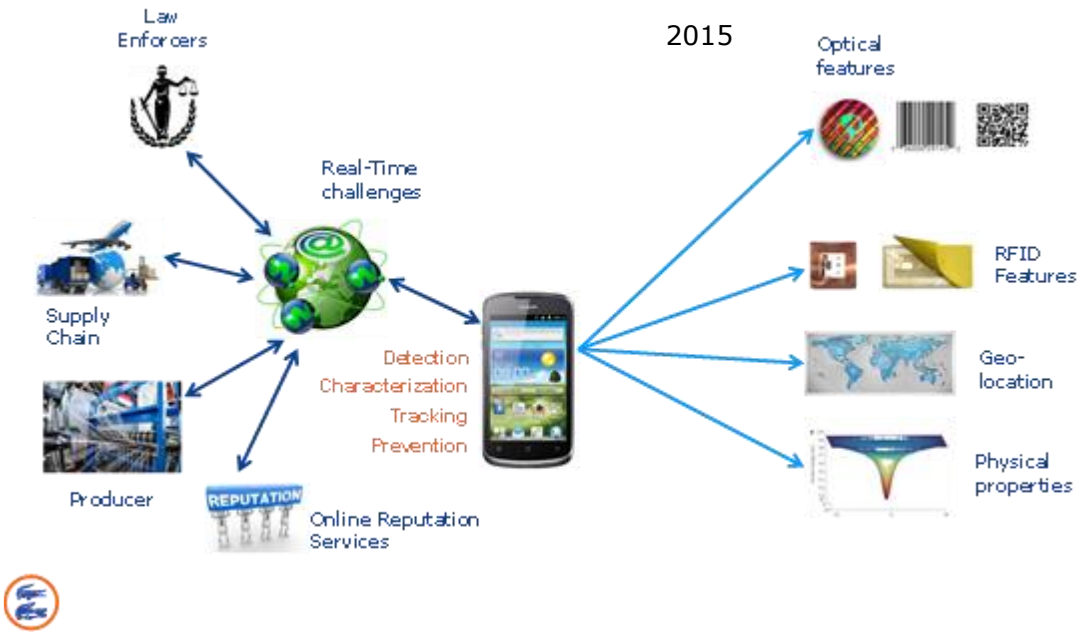
European Commission

JRC TECHNICAL REPORTS

Consumer empowerment in the fight against the counterfeiting of goods and Intellectual Property Rights infringement

Gianmarco Baldini
Igor Nai Fovino

2015



EUR 27703 EN

Joint Research Centre

This publication is a Technical report by the Joint Research Centre, the European Commission's in-house science service. It aims to provide evidence-based scientific support to the European policy-making process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

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

JRC 100009

EUR 27703 EN

ISBN 978-92-79-54587-0

ISSN 1831-9424

doi:10.2788/413023

How to cite: G. Baldini, I. Nai Fovino; Consumer empowerment in the fight against the counterfeiting of goods and Intellectual Property Rights infringement; EUR 27703 EN; doi:10.2788/413023

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), Alessandra Piloni (Italian Consumers Forum) and other representatives from the OHIM Observatory.

Abstract

The objective of this report is provide a survey and analysis of the techniques to empower the consumer in the fight against counterfeiting and IPR infringing products. In this report, the term consumer is used in wide context: consumer can be the generic citizen interested in buying a product, the law enforcer, who want to identify counterfeit goods in the field, a small enterprise evaluating the purchase of a product and so on.

This report focuses on techniques to empower the consumer in the field in the presence of the good itself by using technical tools and devices, which are easily available. The report identifies three main categories of empowering tools. The first category is represented by a modern smartphone (or similar device like a tablet) as a tool to empower the consumer in the fight against counterfeiting. The modern smartphone is equipped with a high resolution camera, support for different standards for wireless connectivity, a powerful processor able to support the implementation of sophisticated algorithms and support for NFC and RFID readers. In addition, the smartphone can be integrated and augmented with a wide range of plug-in devices and tools (e.g., an USB microscope). The second category is represented by a wide range of portable products (e.g., portable spectrometers), which can be used for fight against counterfeiting in the field have also appeared in the market. In many cases, these portable produces implement systems only available in forensic labs. The report will also provide an overview of these systems without entering in the details of the specific product by the specific company. A third category of tools is represented by low cost tools, which are different from the previous categories.

This report provides an analysis of the different needs and levels of competences of the "consumer" and what type of infrastructure must be put in place so that the smartphone/tablet or the portable equipment can be an effective tool. The concept of empowering the consumer can be an important element to support Due Diligence practices and Supply Chain Integrity because the different categories of consumer can authentication the goods in different parts of the supply chain and report the presence of non-compliances (e.g., counterfeit products). Privacy aspects are also taken in consideration. Data collected by a smartphone or the portable equipment may disclose personal information of the consumer. Privacy risks and countermeasures in the specific area of fight against counterfeiting are described.

Finally, this report provides high level recommendations, which are summarized here:

Recommendation 1): A common standard to empower the consumer for good authentication through a smartphone should be developed. In particular the standard should define the generation of unique secured identifiers and the protocols between the smartphone and the remote reference library. Privacy aspects should be taken in consideration.

Recommendation 2): Create an expert group for the analysis of new empowerment techniques appearing in the market.

Recommendation 3): Implement an awareness knowledge management repository at European level in collaboration with retailers and manufacturers to be used and accessed through smartphones.

Recommendation 4): Implement a cost/benefit analysis to implement authentication technology to support empowerment of the consumer in specific domains.

Recommendation 5): In the definition of Due Diligence and Supply Chain Integrity processes to fight against counterfeiting, the role of empowerment of the consumer should be clearly defined.

1. Introduction

This section is used to provide an inventory of the potential technologies, which can be used by a consumer to mitigate counterfeiting and Intellectual Property Rights (IPR) infringements.

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 the distribution of counterfeit goods. The empowerment ranges from simply avoiding being deceived and suffering economic loss to safeguarding the individual from health and life risks. These tools can also be made available to law enforcers. In fact the term consumer is used here in a wide sense: a generic citizen, a law enforcer or a small enterprise can all be consumer (see following sections for a definition of the term consumer).

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 approaches in the soft cluster are quite useful to increase the awareness of the consumer and they are relatively easy to implement, they may not be so effective for the automatic identification of the goods in the fight against counterfeiting. As a consequence, the main focus of this report is on approach belonging to the "hard" cluster where tools (both software and hardware), which are readily available to the consumer, can be used to fight against counterfeiting in the "field". With the term "field", we mean an area distinct from the forensic labs or from the analysis of data collected from supply chains. We mean the physical area where the consumer operates: the shop where a generic citizen buy physical things, or the customs area where the law enforcer operator checks the incoming goods. In other words, the "field" is the physical area where the consumer can see (e.g., visual inspection) or evaluate a good through the tools described in this report.

We can identify three main types of tools and equipment:

1. The first category is represented by a modern smartphone (or similar device like a tablet) as a tool to empower the consumer in the fight against counterfeiting. The modern smartphone is equipped with an high resolution camera (e.g., 5 megapixels and more), support for different standards for wireless connectivity, a powerful processor able to support the implementation of sophisticated algorithms and support for NFC and RFID readers. In addition, the smartphone can be integrated and augmented with a wide range of plug-in devices and tools (e.g., an USB microscope). This category will be the main focus of this report.

2. The second category is represented by a wide range of portable products (e.g., portable spectrometers), which can be used for fight against counterfeiting in the field have also appeared in the market. In many cases, these portable produces implement systems only available in forensic labs until recently. An example is related to portable spectrometers. The report will also provide an overview of these systems without entering in the details of the specific product by the specific company.

3. A third category of tools is represented by low cost tools, which are different from the previous categories. For example, readily available chemical reagents or polarized filters.

The concept of empowering the consumer can be an important element to support Due Diligence practices and Supply Chain Integrity because the different categories of consumer can authentication the goods in different parts of the supply chain and report the presence of non-compliances (e.g., counterfeit products).

The structure of this report is following: section 2 describes the context with the definition of the consumer, the meaning of empowering the consumer and the "field" where the empowering concept is implemented. Section 3 describes the empowerment approach based a smarthphone (category 1 identified above). Section 4 describes the empowerment for categories 2 and 3 identified above. Section 5 identifies the main issues and challenges including privacy aspects. Finally, section 6 concludes this technical report and provide recommendations.

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.

2. Context and definitions

This section provides the operating context and definitions of the terms used in this report.

With the term "empowerment" the "consumer" in the fight against counterfeiting and IPR infringing, we mean an extension of the concept of empowerment the consumer already presented in [1], where it is defined as "empowered consumers need real choices, accurate information, market transparency and the confidence that comes from effective protection and solid rights". The concept of empowerment the consumer is also discussed extensively in market literature to indicate both a subjective state/experience related to an increase in abilities [2] or an objective condition related to greater information or understanding [3][4].

The need to empower the consumers (where the term consumer can have a wide meaning) has been advocated by various sources: from government [5], research [6] and the media [7],[8].

This wide definition of empowerment the consumer can be re-defined in the fight against counterfeiting to empower the consumer to distinguish counterfeit goods from valid ones on the basis of available information, visual inspection and validation through tools "readily" available.

With the term "readily" we mean techniques and tools which are widely available in the market and do not need sophisticated technological solutions and systems or complex training. In other words, the consumer does not need forensic labs tools to distinguish counterfeit goods from valid ones.

The term "technique" is used to describe both technologies and approaches or a combination of both, which can be used in the fight against counterfeiting.

The focus of the report is also on techniques to be used in the "field" where field is the physical area where the consumer operates and where the goods are usually exposed or transiting. In other words, they can be the marketplace or the area where the law enforcer operator checks the incoming goods. In "field", the consumer can see (e.g., visual inspection) or evaluate a good through the tools described in this report. This definition means that we will not explore empowerment of the consumer for e-commerce because the consumer does not have physical access to the good.

The term "consumer" has also a wide meaning and it can include:

1) The generic citizen, who want to purchase a good and (s)he is not sure about the validity of the good (if the good is counterfeit or not).
2) The law enforcer, who want to check the validity of a good in the marketplace or in the customs area.
3) The brand-owner, which wants to check the distribution of counterfeit goods impacting its own brands in the marketplace.
4) An enterprise, which does not have the capabilities to implement sophisticated or expensive controls for the goods provided by the supplier like forensic labs, responsible supply chain management and so on.
5) A retailer or distributor, which want to check that the received good, which much sell or distribute, is not counterfeit.

All these categories can use the empowerment techniques described in this report, but there are some differences among the categories, which are outlined below:

1) The generic citizen has usually limited training and (s)he does not have specific equipment but we assume that (s)he has a smartphone with wireless connectivity.
2) The law enforcer, who want to check the validity of a good in the marketplace or in the customs area. The law enforcer can have specific training to identify counterfeit goods and (s)he may have access to portable equipment beyond a smartphone. The law enforcer can also have access to knowledge database for fight against counterfeiting (examples are the ones provided by WCO, Europol, Interpol and the Observatory by OHIM).
3) The brand-owner, which wants to check the distribution of counterfeit goods impacting its own brands in the marketplace. The brand-owner has usually specific knowledge of its own brand but very limited or no knowledge of the other brands.
4) An enterprise, which does not have the capabilities to implement sophisticated or expensive controls for the goods provided by the supplier like forensic labs, responsible supply chain management and so on. The enterprise has usually specific knowledge of the range of goods used in their business (e.g., electronic components).
5) A retailer or distributor, has also limited training, but he/she can be equipped with specific equipment if it is cost effective, advantageous for his/her activity or it is requested by law.

These differences among the consumers will be taken care in the assessment of the techniques in section 3.

3. Empowering the consumer using a smartphone

3.1 Capabilities of a smartphone

The main concept of this technique using a smartphone. A description of the approach for empowering the consumer using a smartphone is presented in Figure 1.

Figure 1 Empowering the consumer in the fight against counterfeiting of goods with a smartphone

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).

The smartphone can be connected to other systems and components like the Supply chain of the producer, a reference database by law enforcers and other systems.

More precisely, a smartphone (in the current day – December 2015) has the following capabilities:

1) Camera with high resolution. It is now common to have smartphone with camera with 5 Mpixels below 100 Euro and the trend will continue, so we can foresee that new cameras will have even more resolution.
2) Wireless connectivity through different wireless communication standards: WiFi, GSM, UMTS, LTE and with broadband capacity. This ensures that data can be sent in a short time to a remote server (e.g., cloud database) or a remote application.

3) Computing platform with high power. Modern smartphones have similar computing power and capabilities of desktop computers of few years ago and this trend is likely to continue in the future.
4) NFC readers to read High-Frequency (HF) RFID, which operates at the 13.56 MHz frequency.
5) Global Navigation Satellite Systems (GNSS), which can record the time and space when a good is being evaluated.
6) Plug-in of different components through the USB interface. For example, visual augmentation equipment (e.g., USB microscope) or a DVB dongle (e.g., to collect Radio Frequency emission) can be added on a smartphone.
7) Installation and activation of applications on a smartphone, which can implement anti-counterfeiting applications.

Most of these capabilities were not present in phones until recently, so it was relatively difficult to implement anti-counterfeiting techniques. With the new capabilities of a smartphone, it is possible to implement various techniques, which will be described here. This possibility has also been recently reported in the media, see [8],[9] and [10].

In the context of the fight against counterfeiting, the smartphone itself is the component (in the hand of the consumer) of a wider system, which can include an application, a communication protocol, a reference library, a brand-owner database of the product features, or a database linked to the supply chain and other elements.

The smartphone is used to collect data (e.g., images, RFID) from the good to be evaluated, this data can be processed on the smartphone itself (e.g., to extract features) to generate additional information from the raw data using an application. The application sends the data and the information to a remote application using the wireless connectivity and a specific communication/data protocol. Additional information can also be sent from the smartphone like the position of the smartphone if the privacy settings defined by the consumer allows this. The remote application uses a reference library or a supply chain database to match the data and information received from the smartphone. The matching information (i.e., the good is counterfeit) and related data (e.g., for which market the good is produced) is then sent back to the smartphone. Then the application on the smartphone displays this information and data to the consumer. This generic workflow is represented in the following figure:

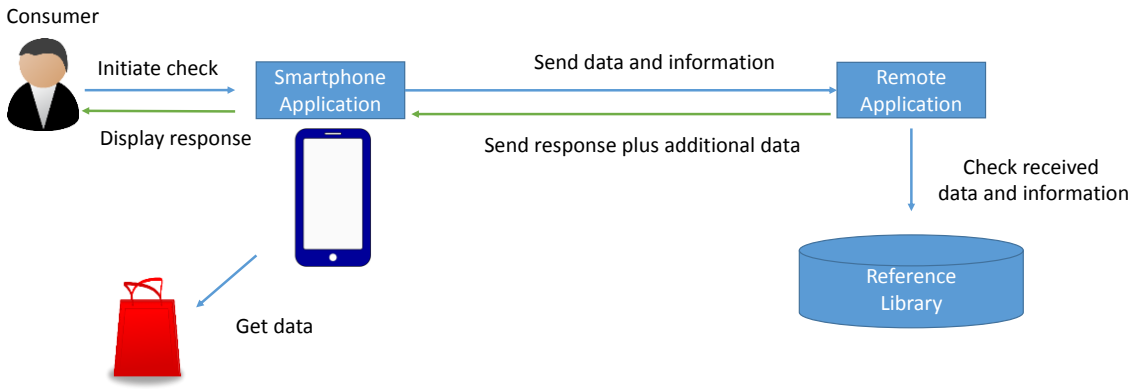


Figure 2 Generic workflow

The consumer only sees the smartphone, but an adequate infrastructure must be put in place to implement the technique for fight against counterfeiting. This is described in the following section.

3.2. Main components of a smartphone-based approach for the fight against counterfeiting of goods

Beyond the smartphone, a complete solution must include the following elements.

1) **Smartphone Application**. This is the application running on a smartphone, which implements a Graphical User Interface (GUI) to the consumer to receive requests. The smartphone is connected to the main sensors of the smartphone to collect the needed data (e.g., images). The application can also implement specific algorithms to process the data. For example, it could extract statistical features from the retrieved image. The smartphone application is also responsible for sending the data and any additional information (e.g., features, position or privacy settings) to the remote application using a well defined communication protocol.
2) **Communication protocol**. This communication protocol is responsible for sending the data and information from the smartphone application to the remote application and sending back the response from the remote application to the smartphone application.
3) **Remote application**. This is the remote application hosted on a remote server, which also uses the communication protocol to exchange data with the smartphone application. The remote application uses the information from a reference library to evaluate if the received data and information from the smartphone identified a *counterfeit* good.
4) **Reference library**. This is the database of the matching information (e.g., track and trace or fingerprinting for goods identifications), which can be created by the brand-owner itself or by an external company which is able to collect from the brand-owner the information identify the valid goods. The reference library is a generic term, which can include many different type of information: it can be the fingerprinting of a good or the serialization number of an over/covert tag. Note that the reference library can also be used to insert additional information useful for the different categories of consumers. For example, the tax regime of a specific market can be inserted in the record of the reference library for a specific good. In this way, the consumer (e.g., law enforcer) can detect a good, which should not be present in the area where it has been evaluated. This capability is very important to counter the threat of smuggling.

3.3. Specific empowerment techniques

We can distinguish different empowerment techniques based on the smartphone, depending how the reference library is created and what type of information is stored or collected by the smartphone:

1) **Reference library created by the brand-owner during the manufacturing process**. The reference library is created by the brand owner itself or by a company working for them and the specific information on the single good is collected and stored in the reference library in the manufacturing phase. In other words, the manufacturing plan of the brand owner is equipped with systems and devices to collect the unique fingerprinting of the good and/or the package, which is then stored for future use. Note that the fingerprinting information can be of different forms: it can be a serial number represented in the bar code or QR code, it can be a fingerprinting of the good itself on the basis of its physical or chemical properties, it can be the RFID applied to the good and/or the package and so on. It can also be a serial number embedded in an overt or cover tag. In fact, a combination of these fingerprinting methods can also be used to improve the authentication accuracy and the resistance to cloning threat of the fingerprinting.

In this case, the reference library must store the correlation of the set of data used to unique identify the package and/or the good.

2) **Reference library created by a commercial third party, which works with the brand-owner.** In this case, the reference library is created by a third party, which works with the brand owner to insert its own tags. The tag is applied on the good after the manufacturing process. As a consequence, it is not an intrinsic property of the good. The difference with the previous case is that a correlation between the tag identifier and the good must be done before the good is distributed in the market. This can increase the risk of cloning or removal of the tag. The advantage is that the brand-owner does not need to invest in the anti-counterfeiting technology if it does not have skill, competences or economic capabilities (e.g., because it is a small company with limited budget) because the commercial third party will do that.

3) **Reference library created by another third party.** In this case, the reference library is created by another party distinct from the brand-owner even if it can collaborate with the brand-owner. For example, the third party can be a consumer association or a law enforcers association, which has collected identification data on specific categories of goods or which would like to create a reference library by collecting and reporting information on potential counterfeit items in the market. For example, it can be aimed to detect counterfeit goods on the basis of specific features: images of ill-formed logos, use of the same identification number in the bar-code, QR code or RFID and so on.

These three techniques will be described in detail in the following sections with details on the technologies, which can be used.

3.3.1. Reference library created by a brand-owner during manufacturing process

In this case, the brand owner collects the data to identify the good in the supply chain or manufacturing process itself. The data can be defined and extracted using different authentication technologies. For example, it can be the specific signature of the paper of a package of cigarette (taken with an image) or it can be the identifier of an RFID embedded in the fabric of a luxury bag.

The choice of the serialization and authentication technology is really dependent on many factors: the type of good, the impact of the authentication technology in the manufacturing process, the associated costs and so on. For many consumer goods, bar codes, QR codes or simple overt/covert technologies can be used, while more sophisticated and expensive goods can use RFID or more complex authentication technologies.

The goal is to collect and store identification and authentication information, which can be correlated with the data extracted by a smartphone in the field. This means that the data generation and collection process in the manufacturing plant must be designed together with the definition of the application in the smartphone or the related protocol.

A pictorial description of the process is provided in Figure 3.

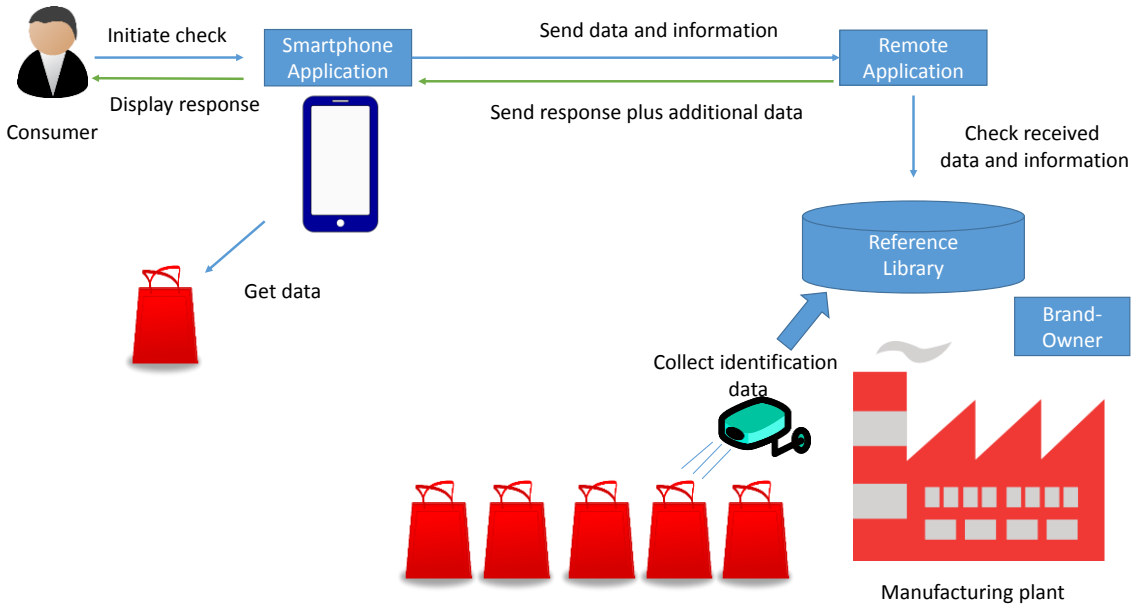


Figure 3 Brand-owner based technique

Supply chain information like tracking and tracing of data can also be used for this purpose if the brand-owner wishes so. 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).

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.

The authentication information can be collected not only on the good itself but also on the packages, storing the goods in a recursive way. In this way, the consumer can have a better traceability of the good, which can also be used to identify gaps in the tracing chain, which can pinpoint to the presence of counterfeit goods.

A good example of this technique is the CODENTIFY [11] developed by Digital Coding & Tracking Association, which represents some of the world's largest manufacturers of tobacco products. As described in [11], CODENTIFY can support:

- Tracking and tracing – enabling electronic monitoring of products as they move forwards through the supply chain and the tracing backwards of their journey history to identify potential points of diversion;
- Product authentication – enabling anyone, anytime, anywhere to immediately verify the authenticity of a product using widely available technologies such as a mobile phone or the internet;
- Digital tax verification – enabling governments to verify and control online the volume of products manufactured and so calculate the commensurate amount of excise and other taxes due.

Currently, CODENTIFY is only used in the tobacco industry and it should be investigated if it can be used in other sectors as well.

Another example, where the intrinsic features of a good taken during the manufacturing process are used to empower the consumer is described in [10]. 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.

NEC notified that the technology is currently in the testing phase and the firm plans to release a commercial version in 2015.

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.

3.3.2. Reference library created by a third party working with a brand-owner

In this case, a commercial third party, which has developed a technology for authentication or track and trace, works together with the brand-owner to apply identifiers tags to the good during the manufacturing process or after the manufacturing process and before the distribution. This case is different from the previous case, because the authentication information (e.g., overt tag) is not an intrinsic part of the good but it is applied to it. Note that the identifier tag could be part of the supply chain integrity process and similar considerations of the open and close supply chain described in 0 do also apply to this case.

The overall workflow is described in Figure 4. The commercial third party applies its own identification and authentication tags to the good after they are produced at the manufacturing plant and before the distribution in the market. The identification and authentication data is then stored in the reference library. Usually, the commercial third party has also developed a remote application and smartphone application to implement the overall workflow.

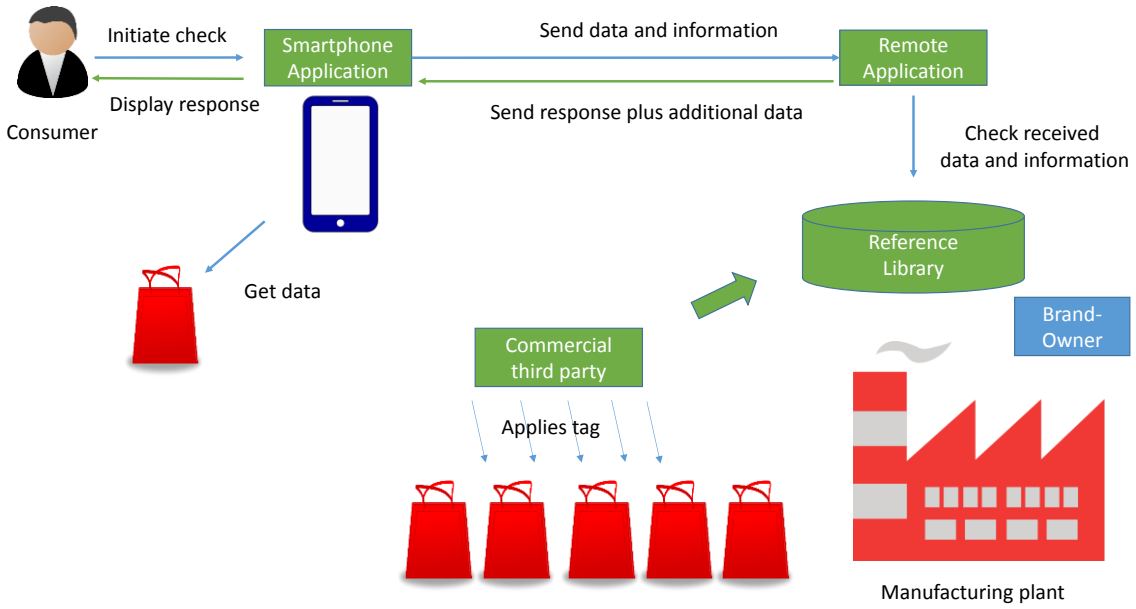


Figure 4 Technique based on brand-owner and third party

This technique is more appropriate for small companies, which cannot afford the implementation of a technique like the one described in 3.3.1. Reference library created by a brand-owner during manufacturing process and for the types of good, where a tag cannot be inserted during the manufacturing plant.

Another advantage of this technique is that the commercial third party, which has developed the technology can create a single smartphone application, a single communication protocol and a single reference library for different categories of goods and brands, thus facilitating the check by the consumer. Obviously, this advantage is also provided by the adoption of a common standard (see the recommendations section 6. Conclusions and Recommendations).

The techniques has been developed by various companies around the world. One example is SICPATRACE from SICPA [12]. In a first phase, called secure marking, the SICPA Data Management System generates a unique reference code for each "unit". This unique reference code can be applied on the good during the manufacturing process. The reference code can include overt, semi-covert and covert features.

Subsequently, each code is activated by SICPA on the production line, thus enabling on-line oversight. With the third stage - distribution control - the codes are scanned as the products move along the supply chain. Each scan sends data to the Data Management System (the equivalent of a reference library) which aggregates details of the product's path until the final point of sale.

Consumers are able to identify and trace products with the SICPAMOBILE® handheld inspection device, which securely authenticates and reads the unique codes.

Other examples are Authenticateit (see [13]), which is a smartphone application that empowers consumers with a fast and convenient way to check an item's authenticity before purchase while offering brand owners a powerful tool to track, trace and prevent instances of unauthorised distribution and retailing. Authenticateit is working with the industry-standard GS1 barcode.

3.3.3. Reference library created by a third party different than brand owners

In this technique, the reference library is created by a third party on the basis of reported information on counterfeit items. For example, a consumer association or law enforcers association can build a knowledge based systems, which includes a reference library to indicate the most common cases of counterfeit items. A consumer can check the validity of the good by sending data about the good to a remote reference library and getting the response or by visually comparing the good with the reference library.

An alternative way is that the consumer provides information to build the reference library or to notify the potential presence of a counterfeit item. One example of this technique is uFaker (see [14]), where a consumer can take a picture of a possible counterfeit items and send this information together with the position to a remote cloud applications, which notifies the brand owners.

An example of the data flow in this technique is shown in:

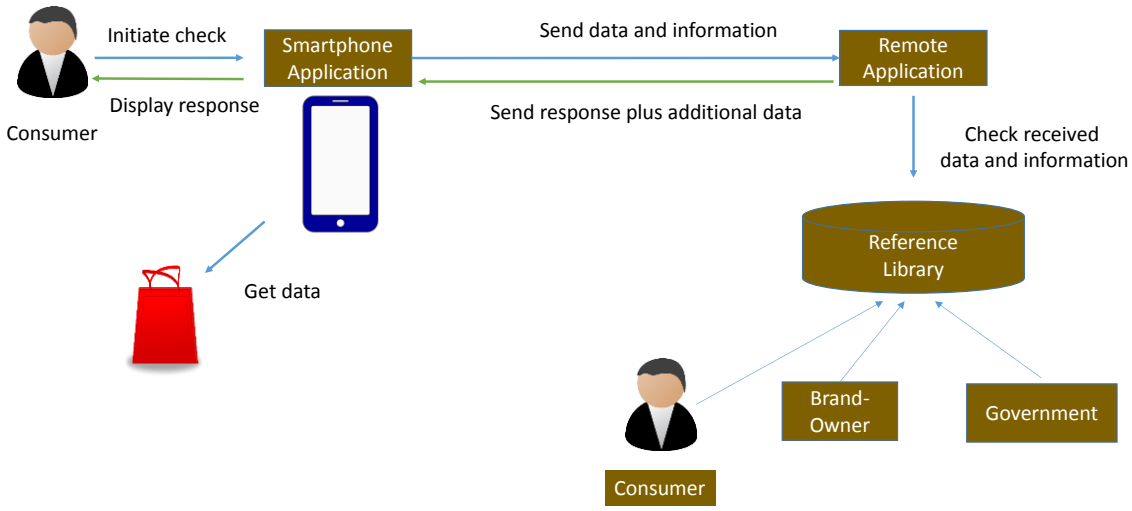


Figure 5 Reference library created by third party other than brand owners

The advantage of this technique is that the reference library can include many different types of goods and brands and it can process and receive input from many difference categories of stakeholders, which can examine counterfeit items in different ways (law enforcers, retailers, distributors, generic citizens and so on).

The disadvantage is that the information stored in the reference library may not be accurate, not complete or not updated. For example, new types of counterfeit goods may not be present in the reference library in time for a proper evaluation.

3.4. Costs analysis.

The costs associated to the design and deployment of anti-counterfeiting solutions for empowerment the consumer using the smartphone are structured in the following way:

1) *Design and implementation of the mobile application*. This is the cost of developing a mobile application, which can be installed on a smartphone and support the solutions of empowering the consumer for the fight against counterfeiting. The application must be designed to interact with the sensors of the smartphone, which are needed to collect the requested data: images, NFC readings, Track and trace information, GNSS position and others.

1) *Reference Library*. This is the cost of developing the reference library, which is used to compare the identification data collected in the field with the database of

identification data stored before the goods are distributed in the market. This costs can also based on different elements: a) the implementation of the means to collect data in the manufacturing or distribution processes, b) the creation of a database to store the reference data, c) development of the remote application to make available and manage the reference library and d) the publication of the reference library on the web to be accessible by the mobile application. Other associated costs like the development of standards, or protocols are described in the other items of this numbered list.

2) *Development of standards*. This is the cost of developing standards for: a) the definition of the protocol between the smartphone and the reference library, b) the format of the data stored in the reference library, c) the serialization coding to identify the good in the reference library, d) 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) *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. As a consequence, one relevant cost can be associated to the integration of the ICT systems used to support the supply chain with the reference library. Note that the integration between the two systems does not need to be complete. In other words not all the data of the supply chain can be used in the reference library as some supply chain data can be proprietary to the brand-owner.

4) *Privacy, security and Access contro*l. This item includes various elements, which addressed the privacy and security aspects of the empowerment concept. Privacy aspects can be quite important for the consumers. If they are not addressed, the deployment of the applications to empower the consumer in the fight against counterfeiting can be hampered because the generic citizen can fear that his/her personal of data is at risk when sending the data of the good. In addition, different categories of consumers (e.g., law enforcers, brand owners) can have different access to the data of the reference library. For example, law enforcers can also use data based on covert features rather than overt features. In addition, access control functions may be needed to ensure that only the reference library can be accessed by the web and not other data systems, which store sensitive information.

3.5. Authentication technologies

This section describes briefly the authentication technologies, which can be used to identify and authentication the goods in the field against a reference library.

Note that a detailed description of the authentication technologies is not in the scope of this report, because such description has already been extensively provided in a previous report drafted by the JRC (JRC98181). Elements of the previous report will be used in this report.

In this section, we focus only on the authentication technologies, which can be supported by the capabilities of the smartphone.

3.5.1. Numeric Identifier/ 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 [15].

There are various examples for the use of the smartphone to read and analyse bar codes so this can be considered a very mature technology.

3.5.2. 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.

There are various examples for the use of the smartphone to read and analyse QR codes so this can be considered a very mature technology.

3.5.3. Physical Fingerprint Technology on visible spectrum

Physical fingerprints use the specific characteristics of the base material or 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.

In this context, we include any physical fingerprint technology regardless of the medium (i.e., material) where it is applied: holograms, paper, inks, security threads and regardless it is overt or covert.

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.

The use of the smartphone to read and analyse physical fingerprint technology is a recent development but it is supported by an increasingly number of companies thanks to the increased resolution of the camera in the smartphone.

There are various examples of companies producing these products, which are listed here not to recommend specifically these products but to show the maturity of this technology:

- VERIFYME (see [17]), where the integration of physical security pigment technologies with digital verification solutions creates an anti-counterfeiting system by which anyone with a smartphone can authenticate material goods. The patented technology uses smart phones in two ways. The phone's internal "flashlight" changes the color of the visible ink identification mark on the package. In addition, the technology leverages the device's camera to detect and recognize a QR code, or similar, invisible mark which is embedded. By communicating with the brand via a special app, the consumer will be assured that the product is genuine, not fake or a cheap, potentially dangerous, knockoff (from [17]).

- Arjo (2015) (see [18]). This company has developed a technology to called Signoptic™, which is is a patented technology based on a vision system converting the texture of a product into a unique signature thanks to a proprietary algorithm. Because the signature is generated from non-duplicable aspects of the product itself, Signoptic™ allows both identification and authentication. Signoptic ™ can be used directly on the product (primary packaging), at the packaging level (secondary packaging) or directly on labels.

- ProofTag (see [19]) has developed various solutions including Ramdot™, which is a security feature based on the dispersion of optical variable particles. In the Ramdot™, particles are scattered in a random manner, thus creating a unique distribution of optically variable elements. The Ramdot™ technology can be applied on several components, such as security seals, shrink sleeves and textile tags. The product can be customized in terms of particles' colors, tactile aspect, and visible metallized effect of the particles. The visual matching of the pattern versus its recorded image allows for an easy identification of the marked object.

Note that these solutions can be both overt or covert and they can be applied both by the brand-owner in the manufacturing process (as described in section 3.3.1. Reference library created by a brand-owner during manufacturing process) or applied to the good in the distribution phase using a tag (as described in section 3.3.2. Reference library created by a third party working with a brand-owner).

3.5.4. Radio Frequency Identifier (RFID)

An RFID tag is basically a device composed of a small chip connected to a coil. 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.

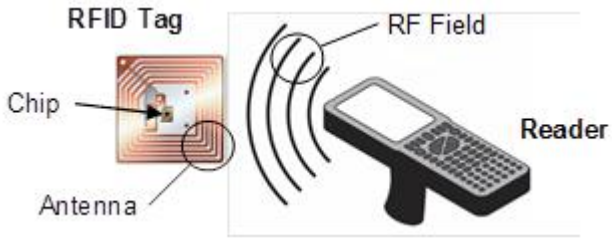


Figure 6 Radio Frequency Id

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.

A smartphone with a NFC reader can read some type of RFID but not all of them, even if various RFID readers connected with USB are available in the market. Passive RFID tags primarily operate at three frequency ranges:

- Low Frequency (LF) 125 -134 kHz
- High Frequency (HF)13.56 MHz
- Ultra High Frequency (UHF) 856 MHz to 960 MHz

Near-field communication devices operate at the same frequency (13.56 MHz) as HF RFID readers and tags. The standards and protocols of the NFC format is based on RFID standards outlined in ISO/IEC 14443, and the basis for parts of ISO/IEC 18092.

The RFID can be inserted in the good if the type of good and its material composition allows that. For example, a RFID can be inserted in the fabric of a luxury bag, but it is more difficult to insert an RFID in a semiconductor chip. In other words, RFID technology can be used both by the brand-owner in the manufacturing process (as described in section 3.3.1. Reference library created by a brand-owner during manufacturing process) or applied to the good in the distribution phase using a tag (as described in section 3.3.2. Reference library created by a third party working with a brand-owner).

3.5.5. 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 [10]. 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.

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.

This technique is slightly different from the technique described in 3.5.3. Physical Fingerprint Technology on visible spectrum because the image captures fingerprints, which have not been inserted on purpose but which are created spontaneously during the manufacturing process. From this point of view, this technology does not need changes to the manufacturing process of the material but it can have less accuracy than the technique described in 3.5.3. Physical Fingerprint Technology on visible spectrum.

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.

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 [20]).

3.5.6. Analysis of the different techniques

The evolution of the technology has paved the way for the use of the smartphone to identify and authenticate goods and distinguish them from counterfeit goods.

In this section, we compare the different techniques to highlight the related advantages/disadvantages.

The techniques based on the unique fingerprinting of the good as described in sections 3.5.3. Physical Fingerprint Technology on visible spectrum and 3.5.5. Collection and analysis of images of the object to be authenticated are more accurate and robust against cloning attacks because it is quite difficult for counterfeiters to reproduce exactly the unique fingerprint of the good. On the other side, it may not be possible to get fingerprints of all different materials using the features of the smartphone. Note that in this section, we are only focused on fingerprints, which can be validated with the basic features of a smartphone as the use of portable devices is described in another section.

Even with these limitations, there is now large variety of products in the market where physical fingerprints can be inserted in common materials used for packaging like paper or special plastics.

The technique described in section 3.5.3. Physical Fingerprint Technology on visible spectrum, where artificial fingerprint are inserted in the good or when a specific material is used to increase the unicity of the good is more efficient than the technique described in section 3.5.5. Collection and analysis of images of the object to be authenticated for obvious reasons: in the former technique, the material is designed to collect unique fingerprints, while in the second technique, the unicity or the preservation of such unicity against change in the environment is not guaranteed. Note that the technique described in section 3.5.3. Physical Fingerprint Technology on visible spectrum can also be used in tags applied to the good or in packaged containing the good.

On the other side, the technique described in section 3.5.5. Collection and analysis of images of the object to be authenticated does not need the application of special solutions in the manufacturing process.

The advantage of the bar-code or QR code described in 3.5.1. Numeric Identifier/ One dimension-Bar Code and 3.5.2. QR code and other two dimensional bar codes is its cost-effectiveness and simplicity. It can be applied on the material using special inks or as a tag. The clearest disadvantage is the clonability as it is relatively easy to reproduce a bar-code or QR code. Clonability threats can be mitigated through the empowerment solution itself: the smartphone can send the identifier of the bar code or QR code to a remote application attached to the reference library, which can checks the presence of duplicated identifiers and inform the consumer about them.

The advantage of bar code/QR code and other overt/covert techniques in comparison to the RFID based technique (described in 3.5.4. Radio Frequency Identifier (RFID)) is the cost of the token itself even if the cost of RFID has decreased considerably in recent times. As described in [21], 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 [4] 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 [21].

Regarding the different categories of consumers, the techniques are mostly transparent to the different categories, even if they can be complemented each other to increase the security for specific classes of consumer categories. In other words, the empowerment technique can be implemented in such a way that the smartphone provides specific data to the generic citizen, other data to the brand owners, to the retailers and the law enforcers. For example, covert data could be used for brand owners and law enforcers while only overt data is used for generic citizens and retailers.

A summary of the analysis is provided in the following tables:

Table 1 Comparison of the empowerment techniques based on the smartphone

Technique	**Cost for the brand-owner**	**Cost for the consumer**	**Market and technical maturity**
Bar Code	Low if the solution is based on an extension of an existing *open-loop* track and trace infrastructure Medium if the solution is based on an extension of an existing *closed-loop* track and trace infrastructure Very high is a new track and trace infrastructure must be created.	Low, because a smartphone can read a bar-code with a simple application, which is already available in the market.	High, because solutions for reading the bar code through the camera of the smartphone are already available.

QR Code	(same as bar code) Low if the solution is based on an extension of an existing *open-loop* track and trace infrastructure Medium if the solution is based on an extension of an existing *closed-loop* track and trace infrastructure Very high is a new track and trace infrastructure must be created.	(same as bar code) Low, because a smartphone can read a bar-code with a simple application, which is already available in the market.	(same as bar code) High, because solutions for reading the bar code through the camera of the smartphone are already available.
Physical Fingerprint Technology on visible spectrum	Medium if infrastructures are not developed yet.	Low because most of the mobile devices have a camera with high resolutions (more than 5 MPixel) and data connectivity should be available.	Medium-High Various solutions are already available in the market as described in the previous sections of the report.
RFID	Low-Medium. Similar considerations apply to RFID as for the bar code and QR codes with the difference that RFID devices are more expensive than bar code and QR code.	Medium, because a modern smartphone should be equipped with a NFC receiver able to support different a specific class of RFIDs. Data connectivity should be available.	Medium-High. RFID track and trace systems are widely available in the market and smartphones are usually equipped with RFID readers even if not for all of the different types of RFIDs.
Collection and analysis of images of the object to be authenticated	Low-Medium if infrastructures are not developed yet. In comparison to "Physical Fingerprint Technology on visible spectrum", the cost is minor because fingerprinting or materials designed on purpose does not be to be used or adopted in the	Low because most of the mobile devices have a camera with high resolutions (more than 5 MPixel) and data connectivity should be available.	Medium because only one development has been proposed by NXP but there are not many products in the market at this moment (end of 2015).

	manufacturing process.		

Table 2 Comparison of the empowerment techniques based on the smartphone for different categories of consumers

Category of consumer	**Bar-Code and QR code**	**Physical Fingerprint Technology on visible spectrum**	**RFID**	**Collection and analysis of images of the object to be authenticated**
Generic Citizen	Smartphone applications on a generic smartphone are available.	Solutions on simple consumer market smartphones are now available, so this technology can be accessible to the generic citizen for identification and authentication of the good.	Modern smartphones can authenticate only a subset of RFID devices using their NFC system. Additional RFID readers, which can be plugged or connected to a smartphone are also available. Still, the generic citizen may not be equipped with such readers in the day by day work. Until technology progresses, the use of RFID for the generic citizen cannot be fully adopted.	A generic application on the smartphone can be easily developed and provided to the generic citizen. Even if the level of accuracy can be less than other techniques (e.g., due to the lack of intrinsic features or lack of specific training of the citizen), it can still provide useful information.
Law enforcer	In comparison to the case of the generic citizen, additional information can be provided only to the law enforcer by the brand-	Similar considerations apply to Bar-Code and QR code considering the maturity of the technology. The difference with the	The law enforcer can be equipped with all RFID plug-in connected to the smartphone. This can become an effective tool for the specific	In comparison to the generic citizen, a law enforcer can have specific training to improve the accuracy in the identification and authentication

	owner from a database associated to the reference library (for example tax information to prevent smuggling)	generic citizen is that a law enforcer can be equipped with a more sophisticated reader than a simple smartphone to detect other features (e.g., covert) features not visible to a generic citizen or a simple smartphone. Additional information can also be provided to the law enforcer (e.g., tax information).	types of products if RFID will be deployed for anti-counterfeiting purposes. In comparison to the case of the generic citizen, additional information can be provided only to the law enforcer by the brand-owner from a database associated to the reference library (for example tax information to prevent smuggling).	of the good. From this point of view, this technique can still provide valid indications to the law enforcers in absence of other information.
Brand-Owner	In comparison to the case of the generic citizen, additional information can be provided only to the brand-owner itself from a database associated to the reference library. This information could be different from the one provided to the law enforcers.	Similar considerations as for the bar-code and QR code with the difference that brand-owners can have special reader to detect covert features.	Employee of the brand owners can be equipped with RFID readers connected to the smartphone to identify and authenticate the product and add information from a database associated to the reference library. This information could be different from the one provided to the law enforcers	The brand owner can have specific training to improve the accuracy in the identification and authentication of the good. As a consequence this techniques can be more effective for brand-owners.
Small Enterprise	In comparison to the case of the generic citizen, additional information	Similar considerations as for the bar-code and QR code.	Employee of the brand owners can be equipped with RFID readers connected to	The limitations in the accuracy or lack of this technique can create issues in the

	can be provided to the small enterprise by the brand-owner from a database associated to the reference library for specific business goals (e.g., premium quality, specific uses)		the smartphone. Similar considerations apply to the bar code and QR code.	establishment of the contractual relationship between the small enterprise and brand-owner. The other techniques could be preferable.
Retailer/Distributor	This can be a similar case of the Small Enterprise.	Similar considerations as for the bar-code and QR code	As in the case of the generic citizen, the retailer must equip himself with a RFID reader connected to the smartphone, which can be a cost not easily supported by the retailers unless requested by regulations.	As in the case of the small enterprise, the limitations in the accuracy can make the other techniques more preferable to this technique. In addition the validation of a good can be more time consuming than the other techniques, which could be an issue for retailers or distributors.

3.6. Awareness through smartphones.

This section describes the implementation of awareness concepts through smartphones.

As described in [22], consumers are not very educated about the ramifications associated with counterfeiting. 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. 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.

A practical implementation of awareness is through the publication of information and data on counterfeit goods on web servers or public knowledge management repositories, which can be accessed by the consumer in the field through smartphones. The advantage of using a smartphone is that the good under evaluation in the field can be directly compared to the data received by the web servers or public knowledge management repositories. For example, the consumer, who want to check if a sport shoe is counterfeit, can search for that model in the knowledge management repository and visually compare it with the shoe. The knowledge management repository can point out that counterfeit sport shoes of that model have a misplaced logo or a different colour of the fabric.

Awareness on the presence and features of counterfeit goods in the market through the smartphone is a simple but effective technique to fight the distribution of counterfeit products for various categories of consumers. Retailers and manufacturers can work together to provide awareness solutions, mobile applications and web sites. To avoid fragmentation of the different solutions and to harmonize the search and presentation of the information needed to identify a counterfeit good, standards and guidelines should be put in place and central knowledge management repository should be set up.

3.7. Findings on empowerment for fight against IP infringing using smartphones.

Techniques using smartphones has now reached maturity and they can be both cost-effective and high accurate in identifying and authenticating a good. These techniques can be applied by the brand-owner as part of the good itself or they can be applied on the good depending on the feasibility of applying intrinsic features.

The smartphone has also the capability with high resolution camera and wireless connectivity to support the various techniques.

One potential issue is the variety of the technical solutions present in the market, which requires a standardization effort to avoid complex validation procedures by the various categories of consumers, which may limit the validity of these techniques. For example, a law enforcer may be obliged to use many different smartphone applications for each technique or brand.

This aspect alone makes unpractical the application of smartphone based solutions for law enforcers and retailer/distributors while it can be effective for brand-owners and enterprise, which work on specific technologies.

A standardization and harmonization process should be established at European level to support the deployment of a single technique (see section 6. Conclusions and Recommendations).

4. Use of a specific portable device, different from a smartphone.

4.1. Introduction

This section analyses the techniques to empower the consumer using portable devices, which can be used in the field to identify and distinguish a genuine product from a counterfeit one. In particular, we investigate the adoption in the field of forensic techniques, which could be possible only in a specialized lab and they are now accessible in portable devices even with some limitations.

With portable device, we mean an electronic device, equipped with sensors, a processing platform and a display. Simpler devices which can be used in the field are discussed in the following section.

In this section, we also analyse the plug in devices, which can connected to the smartphone. The reason, why these devices are addressed here and not in the previous section is that a consumer must still acquire them and carry with them, which can be justified for specific categories of consumers (e.g., law enforcers, enterprise) but not all of them. RFID readers are an exception to this rule, because smartphones are partially supporting them and the trend is to achieve full support in few years.

The status provided in this section is at the moment of writing this report (December 2015). As technology progresses, new devices can appear in the market.

The main categories identified are:

1) Devices for the collection of Radio Frequency signal in space.
2) Portable spectrometers
3) Augmentation devices for smartphones or other IoT devices
4) Simple devices for visual augmentation

4.2. Devices for the collection of Radio Frequency signal in space

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 IP infringing, have specific RF emissions, which distinguish them from valid equipment. This is due to the fact that worst material (i.e., cheap substandard components) or worst manufacturing practices are used to product the electronic equipment at minor costs than the valid equipment. This has been reported by many sources like [23][24].

There are various examples of the application of this technique from literature. For example, [25] show how RF emissions can be used to uniquely identify integrated circuits. In a similar way, [26] 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).

Intrinsic features can also be inserted in the electronic device in the manufacturing process. One example are the Physical Unclonable Functions (PUF), which has also reached market maturity a this stage as they are provided.

The identification of the electronic devices including consumer mass products like smartphones or tables through radio frequency emissions was still a forensic activity until recently. The reasons were based on a) the cost of the radio frequency systems to collect the RF signal in the air, b) the complexity of the algorithms, which was so demanding that specialized hardware was needed c) the training needed to execute such algorithms.

This context has changed with the introduction of new radio frequency front ends and signal processing devices, which have a cost of around 20 euros (e.g., RTL-SDR) and they can be easily plugged in a smarthphone or in a cost-effective portable systems. The processing power of the modern smartphones is such that the execution of sophisticated algorithms can be executed in a matter of seconds for the signal analysis. The RTL-SDR operates in various frequency ranges, which are suitable to the most common wireless communication standards and frequency bands of a mobile device

Note, that RFIDs are also electronic components, Beyond the Id information, the radio frequency signal can also be analyzed to improve the signal identification. In other words, the cloning of the identifier (the ID) in the RFID can be prevented by the analysis of the radio frequency signal.

The adoption of radio frequency analysis as a method to fight against counterfeit products is similar to other methods: it is based on the creation of a reference library, which stores the radio frequency signatures of the electronic devices, which can be collected in the manufacturing process of before the distribution. For example, RF signals can be collected in the standard testing phase, where the transmission/reception capabilities of the smartphone are tested, thus avoiding an additional step in the manufacturing process.

The following elements can be part of this technique:

1) *A Remote database*. A back-end database (e.g., Cloud Computing) should be created with all the fingerprint of RF emissions of the goods to be checked for IP infringing.
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 (e.g., electronic circuit, smartphone).
4) *Radio Frequency receivers.* mobile devices (e.g., smartphones) of the user should be equipped with radio frequency receivers, to collect the RF sample at short range in a wide range of frequencies.
5) *Data connectivity*. User should have access to high speed wireless data link to support the upload of RF fingerprinting to the central cloud even if some pre-processing can be done.

To summarize, this technique is still in the research/prototype phase but it is possible to cost-effective plug-in and simple algorithms processes.

4.3. Portable spectrometers

Various references have described the applicability of portable spectrometers to the fight against counterfeiting especially in the pharmaceutical sector. For example [27] and [28] have reported in their findings on portable spectrometers to identify counterfeit drugs. Here, we mean various types of spectrometers from Raman Spectroscopy to Near

Infrared Spectroscopy (NIRS). Please, see report JRC98181 for a detailed description of the spectroscopy techniques and the application to fight against counterfeiting. In particular [28] has pointed out that "Raman spectroscopy has rapidly evolved over the past 10 years and offers many benefits that include smaller, faster, and portable units that can be very advantageous especially when working to verify counterfeit medicine. This technology is here to stay, and although it brings many advantages, users need to be mindful that the use of portable instruments for counterfeit verification is not without limitations. The degree of uncertainty in the results can be due to spectral features such as S/N, fluorescence, sample properties, or another random variability of the spectral data. The users should consider using more than 1 correlation method and/or spectral technique for product authentication when the result generated by the Raman portable instrument is close to the threshold value (i.e., a p-value of 0.05). The results are not necessarily trust-worthy until further verification is performed".

In a similar way, [27] has stated that "Spectrometers have evolved after having been around for about 50 years now. But, when it was first invented and put together, they were all huge spectrometers that would actually fill up an entire room, believe it or not. And now it has gotten smaller and smaller and smaller to where now spectrometers are the size of a clip-on to your iPhone. In fact, people are now developing apps to really control and maintain and even detect a counterfeit, just by using even your iPhone. Because the iPhone camera flash is becoming the light source for the spectrometer". and "In fact, U.S. Customs and Border Control agencies, along with the FDA, are putting the spectrometers in place everywhere – even in airports where people are trying to smuggle pharmaceutical counterfeits. It is becoming more and more of a well-accepted technology. Even 5-6 years ago when we started, it was not a well-accepted in the industry. But, now it's been well-accepted within all the regulatory bodies in and outside of the U.S".

These views have been confirmed by other sources as well like [29], which reported that "Our new method is built on modified LSLS algorithm and PCA with very small training set. This assay proves to be a successful high-throughput screening approach for hypoglycemics, which involves three types of counterfeit drugs… Firstly, deliberate and time-consuming collection of thousands of authentic drugs, construction and updating of qualitative or quantitative model for every kind of drug could be evaded. Secondly, after all the standard spectra of the commonly-counterfeited APIs have been stored in the spectral database, whichever drug(s) could be calculated promptly to discriminate whether it is counterfeited by any database-stored API(s). Although, the use of Raman spectroscopy for drug detection is not a good choice due to the high energy of the light source and the difficulties in the measurements". The reference by [29] points out to some limitations for the accuracy in the use of portable spectrometers in comparison to the spectrometers in the forensics labs, which is understandable considering the different prices and capabilities of the equipment. Still, the level of accuracy can be adequate for pre-screening, which was confirmed by previous references as well [30].

To summarize, portable spectrometers are now available in the market and various companies offer cost-effective equipment, which can be used by various categories of consumers. While, this may not be applicable to the generic citizen category, law enforcers, enterprise and retail/distributors can use portable spectrometers to pre-screen counterfeit medicines and other materials.

Apart from the decrease in accuracy in comparison to a forensic lab, the limitation of this empowerment technique is its specificity for the pharmaceutical sector and for specific types of medicines. In addition, a similar framework to the other techniques must be put in place, with the following components:

1) *A Remote database*. A back-end database (e.g., Cloud Computing) should be created with the features of the goods (e.g., medicines).
2) *Implementation of the algorithms*: Sophisticated algorithms for pattern matching should be implemented.

3) *Fingerprints collection*: The features of the good (e.g., medicine) should be collected and recorded in the manufacturing phase.

4) *Portable spectrometers.* Portable spectrometers are needed to collect the data in the field.

5) *Data connectivity*. User should have access to high speed wireless data link to support the upload of collected data to the central cloud even if some pre-processing can be done.

4.4. Augmentation devices for smartphones or other IoT devices

Other augmentation devices are also available for smartphones. One of the most common and simple is an USB magnifier, which can be connected to the smartphone or a computer. This simple tool can be used to improve the visual capabilities of the consumer to inspect a potential counterfeit good. Other components

The application of USB microscopes, which provide the image directly to a computer has been mentioned in [31] 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 [32].

More powerful tools have been researched and developed by DARPA as described in [33]. 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.

Another category of equipment is based on reality augmentation devices like Google Glass. An example of the application of Google Glass for fight against counterfeiting is provided here.

4.5. Use of simple devices

In this section, we describe the availability of simple devices, which appeared recently in the market. With the term "simple devices" we mean cost-effective tools, which can be used in simple way (e.g., no training or very basic training) and which are not in the previous categories (e.g., smartphone or portable spectrometers).

Example of "simple devices" are:

1) Ultraviolet light detector, where the equipment shines an ultraviolet light against the surface of a good or a package to highlight embedded features placed before.

2) 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 or from research [34].

3) Thin-layer chromatography, which can be used for medicines [35]. is a chromatography technique used to separate non-volatile mixtures. Thin-layer chromatography is performed on a sheet of glass, plastic, or aluminium foil, which is coated with a thin layer of adsorbent material, usually silica gel,

aluminium oxide, or cellulose. They can be employed for the identification of drug substances, the estimation of drug substance content and the detection of related substances which could be regarded as impurities. Note that thin-layer chromatography can only be applied where a chemical reaction is used to identify the good (e.g., medicine sample).

Other techniques can be developed in the future, so the previous list is not exhaustive.

All these techniques require very simple tools to carry or to buy and a low level of training (apart from thin-layer chromatography). While technique 3 is for specific types of goods where the chemical composition of the good must be assessed (e.g., pharmaceutical products), the first two techniques can be applied directly to labels applied to the goods and package.

The main advantage of these techniques (especially 1 and 2) is simplicity, low cost, no need of remote connectivity, low level of requested training and portability of the item (a strip to apply Latentogram is only few cms long and weight tens of grams). The potential disadvantage is that it can be mostly used for authentication of the good rather than identification or to get additional information from a remote reference library. Still, they can be an effective instrument in the fight against counterfeiting.

4.6. Findings on empowerment using specific portable devices, different from a smartphone

Different types of analysis apply to the different categories presented in the previous sections

1) Devices for the collection of Radio Frequency signal in space.
2) Portable spectrometers
3) Augmentation devices for smartphones or other IoT devices
4) Simple devices

The first category is still in the research/prototype phase even if it is indeed possible with the current available technologies. Still its market deployment is not happened at the time of writing this report. For some categories of consumers, some training is also needed to capture in the appropriate way the Radio Frequency signal in space. A strong limitation of this technique is that it can be used only for a specific category of goods.

Portable Spectrometers started to be available in the market and some categories of users like law enforcers or brand owners can use them to distinguish between valid goods and counterfeit goods. While the market availability is certainly better than the first category, some training is still needed to analyse the good in an effective way. The need of such training can limit the applicability of this technique to trained law enforcers and brand-owners which presumably are familiar with the technique. Portable spectrometers can be quite accurate for very specific categories of goods, but it is not appropriate for many other categories of goods.

The third category can be the most appropriate when the technology can be relatively simple to use as in the case of a USB microscope or when the device itself can automate the identification as in the case of Google Glass. The evolution of IoT and augmented reality devices can indeed automate solutions for fight against counterfeiting and this is an important trend to consider.

The fourth category can be quite simple to adopt and it can be used for a large variety of categories including packaged goods. The limitations are that it mostly provides identification and authentication but not detailed information on the good because it does not connect to a reference library and an associated database. For example, tax information would be difficult to implement. Still, this category of techniques can be a simple and valid tool for authenticating the goods.

The analysis presented above is summarized in the following table:

Table 3 Summary of the analysis

	Devices for the collection of Radio Frequency signal in space	**Portable spectrometers**	**Augmentation devices for smartphones or other IoT devices (evaluation for the simplest techniques)**	**Use of simple devices**
Cost	Medium	High	Low-Medium	Very Low
Technological Complexity	Medium	Medium-High	Low	Low
Level of Training Needed	High	Medium-High	Low-Medium	Low
Market Maturity	Low	Medium-High	High	High
Categories, which can benefit	Citizen: Low Law Enforcer: Low-Medium Brand-Owner: Medium-High Enterprise: Medium Retailer/Distributor: Low	Citizen: Low Law Enforcer: Medium Brand-Owner: Medium-High Enterprise: Medium Retailer/Distributor: Low	Citizen: Medium Law Enforcer: High Brand-Owner: High Enterprise: Medium Retailer/Distributor: Low-Medium	Citizen: Medium Law Enforcer: High Brand-Owner: High Enterprise: High Retailer/Distributor: High

5. Issues and challenges for empowerment

5.1. Privacy aspects

This section addresses the problem of the privacy of the consumer in the context of empowering the consumer. This issue can potentially impact only the category of the generic citizen as the other categories will use the empowerment techniques as part of his/her professional role. Instead, the generic citizen may be rightfully worried that the empowering technique can provide personal data together with the data sent to the remote application to check if the good is counterfeit.

In fact, privacy aspects can be easily addressed using the two following privacy protection techniques in the design of the application on the smartphone:

1. Application of anonymization technology before sending the data to the remote application to check if the good is counterfeit. With the term anonymization, we mean the process to make the data sent to the remote application anonymous regarding the identity of the consumer. For example, the identity of the user of the smartphone or other identifying data (e.g., location) is removed from the set of transmitted data.
2. Use of informed consent. In this case, the consumer accepts that the transmitted data contains personal information through informed consent, which is registered electronically on the smartphone and it is sent together with the application data. The consumer can provide informed consent for various reasons. For example, the application (here you have to refer to the application, which gives prizes for counterfeiters), gives prizes to consumer, who report a counterfeit item. In this case, the consumer can voluntarily provide identification information.

More sophisticated Privacy Enhancing Technologies (PET) can be used to protect the privacy rights of the citizens, but these technologies comes at a cost.

The economics related to the deployment of PET or more sophisticated forms of Informed Consent can be indeed an obstacle to the deployment of empowerment techniques for fight against counterfeiting. In case, the recommendation is to adopt simple PET, which are already available in the market for the design of the application to empower the consumer. We highlight again that the protection of privacy rights basically applies only to one category of consumer.

5.2. Market fragmentation

This report and other reports on technologies for fight against counterfeiting have clearly shown that there are many empowering technologies present in the market. Such technologies can use the smartphone, which is today a consumer mass market device (and whose cost will decrease even further in the future) or other devices simpler or more sophisticated. We claim that the new set of technologies and applications can support fight against counterfeiting in a more effective way that in previous years.

Beyond these positive developments, one significant issue is the variety of techniques in the different domains and sectors, which can become an hurdle for the consumers, which belong to the professional categories of law enforcers and retailer/distributors.

While brand owners and enterprises work on their specific sectors and they may adopt only one or few empowerment techniques, law enforcers have to evaluate many different types of goods in the daily activities. The availability of many different

empowerment techniques and applications may become an hindrance rather than an effective supporting tool, because law enforcers will have to use a separate technique for different types of goods and even different types of brands. It is easy to imagine that such approach would not be practical and it may have a negative impact the deployment of empowerment techniques in the law enforcer community and in other categories as well (e.g., retailer/distributors). The generic citizen can also be adversely impacted by the availability of empowerment techniques, but for this category, the adoption of these techniques is on voluntary basis rather requested by the professional activities. Thus, it can be less relevant.

Actions must be taken to support the law enforcer and the retailer/distributor to overcome these issues. Various approaches are possible:

1) A common standard for identification and authentication is defined for brands belonging to the same sector or across different sectors. Then, applications are developed on the basis of this standard in such a way that a single application is able to evaluate goods of different brands in a specific sectors. While, this is not an easy task, there are already standardization efforts in place, which can be a valid basis for further development (REF).
2) An international and operational organization, which takes the responsibility of harmonizing and unifying the different authentication technologies. One example of this solution is IPM Connected by the WCO, which is one of the largest and most effective implementation of technical means to fight against counterfeiting. As described in [36], IPM addresses two main goals: a) the possibility to use mobile devices to scan barcodes found on millions of products, b) 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.

5.3. Training

The various empowerment techniques presented in this report do require some level of training, which can range from low in the case of the smartphones reading a bar code, to relatively high in the case of portable spectrometers.

Training and the knowledge on how to use the empowerment technique is an important element in the successful deployment of empowerment techniques because lack of training can decrease the accuracy in the identification of the good. Lack of accuracy and the consequent frustration of the consumers in using the techniques can lead very soon to a rejection of the empowerment technique. Training should be provided by the companies (e.g., brand-owners) or technological implementers of the technique.

The operational effort to develop training practices for the empowerment solutions can be considerable and it is preferable that the empowerment techniques are developed automatic support mechanisms. For example, a wizard or an automated sequence of steps is implemented to guide the consumer in the proper acquisition of data of the good.

6. Conclusions and Recommendations

In this section, we identify the main recommendations, which are based on the analysis provided in the previous sections.

6.1. Standardization of the authentication technique for empowering the consumer

The presence of many technological solutions in the market to empower the consumers in the fight against counterfeiting and IPRs infringing using smartphones shows that the techniques described in 3.3.1. Reference library created by a brand-owner during manufacturing process and 3.3.2. Reference library created by a third party working with a brand-owner are now mature and they are cost efficient. On the other side, the presence of many different solutions creates an obstacle to deployment of this technique as the consumer need to use many different applications for different sectors and even different brands in the same sector. It is recommended to support a standardization activity to select and develop a single standard to support the good authentication and tracking and tracing the goods. We also recommend to use as a starting point CODENTIFY by DCTA (Digital Coding and Tracking Association) and to involve the ISO standardization technical committee ISO/TC 246, Anti-counterfeiting tools. An alternative way is to nominate a central organization responsible for the harmonization of empowerment techniques. An example is the IPM Connected program by the WCO, which is specific for custom officers, but it can be expanded to other categories.

Recommendation 1): A common standard to empower the consumer for good authentication through the smartphone should be developed. In particular the standard should define the generation of unique secured identifiers and the protocols between the smartphone and the remote reference library. Privacy aspects should be taken in consideration.

6.2. Creation of an expert group on the empowerment of the consumer

Various technologies are created every year in the market to identify and authenticate goods through smartphone and other portable instruments. Each technique can be appropriated for specific domains. An expert group should be created to investigate and analyze every year the new solutions in the market and evaluate the applicability in various domains. This activity can be linked to the standardization activity described in the previous recommendation in section 6.1. The export group should be composed by manufacturers, retailers, distributors, law enforcers, developers of anti-counterfeit solutions, government representatives and consumers associations.

Recommendation 2): Create an expert group for the analysis of new empowerment techniques appearing in the market.

6.3. Definition of an awareness program to detect the counterfeit goods through a smartphone

Awareness on the presence and features of counterfeit goods in the market through a smartphone is a simple but effective technique to fight the distribution of counterfeit products for various categories of consumers. Retailers and manufacturers can work together to provide awareness solutions, mobile applications and web sites. To avoid fragmentation of the different solutions and to harmonize the search and presentation of the information needed to identify a counterfeit good, standards and guidelines should be put in place and central knowledge management repository should be set up. In Europe, the Office for Harmonization in the Internal Market (OHIM) could have a role to implement the central knowledge management repository through the Observatory.

Recommendation 3): Implement an awareness knowledge management repository at European level in collaboration with retailers and manufacturers to be used and accessed through smartphones.

6.4. Establishment of links between Due Diligence/Supply Chain Integrity and Empowerment of the Consumer

Most of the empowerment techniques described in this report require the establishment of a reference library based on supply chain information. On the other side, empowerment solutions can support the implementation of Due Diligence and Supply Chain Integrity, because they enable check points in the supply chain. To support the empowerment of the consumer, manufacturers should include authentication technology in the product design and manufacturing processes (see also [37]). 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. In the cost benefit analysis, the application of simple devices (described in section 0) against smartphone and portable equipment should be evaluated. These considerations lead to two following recommendations:

Recommendation 4): Implement a cost/benefit analysis to implement authentication technology to support empowerment of the consumer in specific domains.

Recommendation 5): In the definition of Due Diligence and Supply Chain Integrity processes to fight against counterfeiting, the role of empowerment of the consumer should be clearly defined.

References

[1]. EC (2007). Consumer Policy Strategy 2007-2013, 'Empowering consumers, enhancing their welfare, effectively protecting them' (COM(2007) 99 final).

[2]. Wathieu, L., et al. (2002). Consumer Control and Empowerment: A Primer. Marketing. Letters, 13(3), 297-305.

[3]. Brennan, C.,Ritters, K.(2004). Consumer Education in the UK: New Developments in Policy, Strategy, and Implementation. International Journal of Consumer Studies, 28 (March), 97-107.

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

[5]. Rust, R., Oliver, R. (1994). Video Dial Tone – The New World of Services Marketing. Journal of Services Marketing, 8 (3), 5-16.

[6]. Phuc (2015). Deputy PM Phuc urges promoting community empowerment in fighting against counterfeiting. http://en.nhandan.org.vn/society/legal/item/3430702-deputy-pm-phuc-urges-promoting-community-empowerment-in-fighting-against-counterfeiting.html. Last accessed 15 December 2015.

[7]. Miliard (2012). Rx anti-counterfeiting technologies to reach $1.2B by 2015. http://www.healthcareitnews.com/news/rx-anti-counterfeiting-technologies-reach-12b-2015. Last Accessed 15 December 2015.

[8]. WTMR (2014) Anti-counterfeiting apps on the rise, but consumer take-up remains a challenge. http://www.worldtrademarkreview.com/Blog/detail.aspx?g=31c7fd36-3aca-4fb9-aae6-ea75428e852e.

[9]. Bilcare 2015 Smart Devices by Adrian Burden at BilcareTechnologies http://www.bilcaretech.com/pdf/whitepaper/Technology-has-a-habit-of-converging.pdf. Last accessed August 2015.

[10]. PC World. NEC smartphone tech can spot counterfeit goods http://www.pcworld.idg.com.au/article/559250/nec-smartphone-tech-can-spot-counterfeit-goods/. 10 November 2014.

[11]. CODENTIFY 2015. http://www.dcta-global.com/our-mission.html. Last accessed 12 December 2015.

[12]. SICPATRACE (2015). http://www.sicpa.com/government-security-solutions/sicpatrace. Last accessed 2 December 2015.

[13]. AUTHENTICATEIT (2015). http://authenticateit.com/. Last accessed 2 December 2015.

[14]. uFaker (2015). https://www.ufaker.com/. Last accessed 2 December 2015.

[15]. GS1 http://www.gs1.org/docs/barcodes/GS1_General_Specifications.pdf. Last accessed 2 December 2015.

[16]. (ATT 2015) Seal Vector. www.att-fr.com . Last Accessed 12 December 2015.

[17]. VERIFYME (2015). http://www.verifyme.com/new-blog/2015/9/22/verifyme-receives-notice-of-allowance-for-authenticating-security-marks-on-material-goods-with-a-smartphone-app

[18]. Arjo (2015). http://www.arjo-solutions.com/en/. Last accessed 2 December 2015

[19]. ProofTag (2015). http://www.prooftag.net/solutions-2/authentication-technologies/. Last accessed 2 December 2015.

[20]. Rytter, W. (2000). Compressed and fully compressed pattern matching in one and two dimensions. Proceedings of the IEEE, 88(11), 1769-1778.

[21]. 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
[22]. Anne E. Wilcock, Kathryn A. Boys, (2014) 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.
[23]. 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 12 December 2015.
[24]. NOKOMIS (2014) http://www.nokomisinc.com/. Last accessed 12 December 2015.
[25]. 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.
[26]. 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.
[27]. Kalyanaraman, R., (2015). Counterfeit or Not? Use a Spectrometer to Find Out. Anti-counterfeiting for Pharmaceutical and Medical Devices. http://www.anticounterfeitingpharma.com. Last Accessed 15 December 2015.
[28]. Anna Luczak, PhD , Ravi Kalyanaraman, Ph.D. (2014). Portable and Benchtop Raman Technologies for Product Authentication and Counterfeit Detection http://www.americanpharmaceuticalreview.com/Featured-Articles/169505-Portable-and-Benchtop-Raman-Technologies-for-Product-Authentication-and-Counterfeit-Detection/. Last Accessed 16 December 2015.
[29]. Feng Lu (2013), Xinxin Weng, Yifeng Chai, Yongjian Yang, Yinjia Yu, Gengli Duan, A novel identification system for counterfeit drugs based on portable Raman spectroscopy, Chemometrics and Intelligent Laboratory Systems, Volume 127, 15 August 2013, Pages 63-69, ISSN 0169-7439, http://dx.doi.org/10.1016/j.chemolab.2013.06.001.
[30]. O'Neil, R. Jee, G. Lee, A. Charvill and A. Moffat, (2008) "Use of a portable near infrared spectrometer for the authentication of tablets and the detection of counterfeit versions", J. Near Infrared Spectrosc. 16(3), 327–333 (2008)
[31]. Villasenor, J., & Tehranipoor, M. (2013). Chop shop electronics. Spectrum, IEEE, 50(10), 41-45.
[32]. AERI 2015. Counterfeit Electronic Component Detection. http://www.aeri.com/counterfeit-electronic-component-detection/ Last Accessed 3/07/2015.
[33]. 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.
[34]. Müller, C. and Garriga, M. and Campoy-Quiles, M. (2012). Patterned optical anisotropy in woven conjugated polymer systems, Applied Physics Letters, 101, 171907 (2012), DOI:http://dx.doi.org/10.1063/1.4764518.
[35]. WHO 1999. Counterfeit Drugs. Guidelines for the development of measures to combat counterfeit drugs.
[36]. WCO (2105). IPM Connected http://www.wcoipm.org/ipm-connected. Last accessed 10 August 2015.
[37]. GMA 2014. Grocery Manufacturers Association. Brand Protection and Supply Chain Integrity: Methods for Counterfeit Detection, Prevention and Deterrence A Best Practices Guide http://www.gmaonline.org/filemanager/Collaborating_with_Retailers/GMA_Inmar_Brand_Protection.pdf. Last accessed 12 December 2015.

List of abbreviations and definitions

CCP	Customs Organization Global Container Control Programme (CCP)
COAs	Certificate Of Authenticity (COAs)
COAs	Privilege Management Infrastructure (COAs)
EDS	Electron Dispersive Spectroscopy
EPC	EPC (electronic product code).
FTIR	Fourier Transform Infrared Spectroscopy
GNSS	Global Navigation Satellite Systems
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
PET	Privacy Enhancing Technology
PUF	Physical Unclonable Function
RFID	Radio Frequency Identifier
SAM	Scanning Acoustic Microscopy
SEM	Scanning Electron Microscopy
TGA	Thermogravimetric Analysis
UHF	Ultra High Frequency
UV	Ultra-Violet

WHO	World Health Organization

List of figures

List of tables

How to obtain EU publications

Our publications are available from EU Bookshop (http://bookshop.europa.eu),
where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents.
You can obtain their contact details by sending a fax to (352) 29 29-42758.

LB-NA-27703-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

doi:10.2788/413023

ISBN 978-92-79-54587-0