COALITION AGAINST ILLICIT TRADE

Governance and Data Management for Cross-border

Tracking, Tracing and Authentication Systems

To combat Illicit Trade and Counterfeiting

06 December 2016

Contents

01 Introduction

The occurrence of cross-border illicit trade and seizures of counterfeit goods by EU authorities continues to rise year on year. The OECD and the EU's Intellectual Property Office (EUIPO) estimate that imports of counterfeit and pirated goods are worth nearly half a trillion dollars a year, or around 2.5% of global imports, with US, Italian and French brands the hardest hit. What is more, much of the proceeds of this activity go to organised crime[1].

As revealed by the latest sectorial report of EUIPO, fake medicines alone cost the EU pharmaceutical sector €10.2 billion each year[2]. According to a 2016 report by the European Commission, intercepted goods by EU customs authorities in 2015 grew by 15% compared to the previous year[3]. More than 40 million products suspected of violating an intellectual property right were detained at the EU's external borders, with a total value of nearly €650 million. According to this report, China was the main country from which counterfeit goods originate accounting for 41% of such products, followed by Montenegro, Hong Kong, Malaysia and Benin.

Manufacturers of almost all mass-produced and high-value niche products, be it food, beverages, drugs, tobacco, electronics, mechanical spare parts, cosmetics, toys, crops or jewellery, have been operating coding systems for several years now with the aim of ensuring traceability and testifying to the authenticity of their product. Existing tracking, tracing and authentification (TT&A) systems, and those that emerge from new technological developments, support manufacturers, logistics companies and public authorities across the EU and globally in the fight against counterfeiting and illicit trade. Their widespread adoption and operational effectiveness is driven by a number of technical, organisational and policy decisions involving both operators and public authorities which can determine the success or the failure of the system.

This paper, a collaborative report by members of the Coalition Against Illicit Trade[4], aims to address these drivers from the perspective of experienced service providers, whose hands-on experience has allowed them to identify the barriers to and the enabling conditions for the adoption of innovative solutions matching business and public policy needs. It should be seen as a work-in-progress contribution that will hopefully encourage further exchange and more informed decisions by policy makers and businesses in this area.

[1] Report on Trade in Counterfeit and Pirated Goods. Mapping the Economic Impact, OECD, Paris, 2016.

[2] The economic cost of IPR infringement in the pharmaceutical sector, EUIPO, 2016. The report is the ninth in a series of studies undertaken by EUIPO into the economic impact of counterfeiting in industrial sectors in the EU. The series previously looked at: the spirits and wine sector; the recorded music sector; the watches and jewellery sector; the handbag and luggage sector; the toys and games sector; the sports goods sector; the clothes, shoes and accessories sector; and the cosmetics and personal care sector.

[3] Report on EU customs enforcement of intellectual property rights: results at the EU border 2015, Brussels, 2016

[4] CAIT members includes Aegate, Atos Worldline, ArjoSolutions, Domino, Essentra, FATA Logistic Systems, Fracturecode, Nano4U, Scan Trust and Viditrust. For more information visit http://www.coalitionagainstillicittrade.org/

02 Critical factors governing a TT&A system: determining responsibility and accountability

There are two underlying factors which determine the effectiveness of a TT&A system as a whole: the technical standards under which the system is engineered and the equipment required to operate the system along the supply chain from production to retail.

THE ROLE OF BUSINESS

Manufacturers and other economic operators intervening in the supply chain are well placed to select the best emerging technology available. They can most accurately judge which equipment matches their economic and safety objectives, without unduly disrupting the production and distribution flow from origin to market. Moreover, the architecture of the system and the equipment chosen should allow control by local public authorities for health and safety, taxation and customs purposes.

An effective T&T system allows the identification of the point of potential diversion of legitimate products in the supply chain. The application of unique identifiers to each product or pack of products is an enabler of T&T processes by making every pack unique and thus traceable. Provided that the unique identifier is generated in accordance with random generation rules and is encoded using standard data structure and syntax, the nature of the originator of such code is not relevant for T&T purposes.

For practical reasons, it can be within the remit of the brand owner, manufacturer or any third-party service provider designated by the brand owner for this purpose. In addition it should be noted that, though the role of T&T is not to ensure production control per se, when there is a legal obligation for a manufacturer to mark and scan all of his products with a unique identifier, this provides law enforcement authorities with the ability to discover whether the manufacturer has a hidden production capacity, notably in the case of excisable products.

Commercially relevant and competitive solutions operated by the industry will ensure that deployment is rigorously assessed, that the most cost-effective solution is used, and that the impact on the cost to end consumers and businesses is minimized.

THE ROLE OF PUBLIC AUTHORITIES

Public authorities, regulators and independent standard setting bodies have a crucial role in defining TT&A standards in order to ensure the interoperability of the system, especially across borders. However, the prescriptive character of standards should not jeopardize a competitive level playing field for suppliers by creating monopolistic market segments that reduce the cost-effectiveness of the solutions deployed and disincentivise innovation.

Public authorities should focus on what they want to achieve from a political and regulatory perspective, rather than dictating the technological means to reach the policy objectives. The initial failure of the United States with its pharmaceutical anti-counterfeiting measures back in the early 2000s should serve as a warning. The original idea was to create a major FDA-controlled collaborative system that would require RFID chips to be placed in every pharmaceutical package, with a designated IT company to champion the software side. The project collapsed after about two and a half years because pharmaceutical industry constituents largely did not buy in. The new US regulation, that enters implementation (stage 1) at the end of 2017,

now largely refrains from defining technological solutions and industry is already conforming to this legislation more than a year in advance of the deadline – with a number of different technical (but legally compatible) solutions already in the marketplace.

In summary, public authorities at the national and international level, when addressing policy recommendation and statutory requirements, should take the following into consideration:

- Identifying methodological standards for applying TT&A to production-supply chain processes, although these may be product-specific.
- Defining technical standards only for basic elements of the TT&A process.
- Applying defined standards uniformly to the products to be tracked, traced and authenticated.
- Allowing producers and supply chain operators to select the most appropriate technologies to fulfil TT&A standards, that best fit their respective industrial environments.
- Allowing outsourcing of the TT&A applications to "certified" third parties.
- Promoting competition and innovation through the establishment of an accreditation/ certification mechanism for systems deemed compliant with the regulatory requirements or the internationally agreed standards both for the provision of data and technical standards, irrespective of the technology providers.
- Promoting overarching technological architectures, which would enable interoperability across different technological platforms, geographies and industry sectors.
- Assessing and benchmarking the cost effectiveness of optional solutions taking into account the value of the products they "protect" and the industry specific objectives in tracking and tracing.
- Considering the affordability of initial TT&A investments required for every company and operator in a given industry and market sector, with a view to avoid discriminatory entry barriers for companies due to lack of investment capabilities.

THE ROLE OF THE SYSTEM CONTROLLER

The first level of control of any tracking and tracing system is, of course, performed by the brand owners themselves who have every interest in securing their own supply chains, stopping diversion of their products from the legitimate distribution chain and exclude the possibility of counterfeit products being substituted for their own genuine products.

Also all other participants in the supply chain have a responsibility to collaborate and ensure that their part in the overall chain is secure by accurately logging and transmitting all necessary data on the movement of the products.

Meanwhile, a secure system is never built on trust alone, and certainly for regulated products, it is up to the public authorities or the standard-setting bodies to safeguard the integrity of tracking and tracing systems, to ensure transparency of operation of manufacturers and to ensure adequate outside controls and audits by third parties accepted by relevant authorities or standard-setting bodies.

By setting an open specification which determines the purpose and the function of the TT&A solution, regulatory bodies can define the terms of reference for external audits of compliance and effectiveness of the systems and solutions chosen by industry. Where an industry-developed and operated solution is an option, external control and oversight can be easily achieved through clear and agreed standard operating procedures (SOPs). Clear SOPs can be monitored and audited on a regular (or irregular) basis to ensure economic operators are compliant with the policy objectives.

03 Data flows and storage

SCOPE OF DATABASE CONTENT

Policy makers should define the nature of data to be collected for their own legitimate policy objectives in standard TT&A databases, and leave the responsibility of that data management to the owners, while requiring relevant transmission to external TT&A databases.

Each industry sector concerned should be consulted on how to define which information should be collected and stored along the supply chain and made accessible to relevant authorities intervening in the supply chain under the control of independent certified service providers.

DATABASE MANAGEMENT

The brand owner is responsible for the "protection" of his own distribution chain. It follows that brand owners should be able to consult all data on their own products in the databases, in order to spot potential weaknesses or diversions in their supply chain.

To avoid issues of access to confidential data by competitors and liability in case of technical failures, the most logical set-up would be to have a database per manufacturer or brand owner where data is stored locally.

Where appropriate, these databases could be controlled by an independent operator acting in coordination with relevant public authorities and supporting them in their controlling activity.

Experience with the implementation of the Falsified Medicines Directive at EU level shows that it is difficult to make national code management centres responsible as gate-keepers of data-flows. This approach is prone to technical failure, as the number of codes quickly becomes overwhelming and data errors often lead to perfectly good products being sent back to manufacturers. In the case of high-value goods, this can lead to significant costs, pushing manufacturers to look for alternative authentication solutions.

All information relevant for law enforcement and national authorities could be transmitted from such brand owner databases to external TT&A databases, access to which would be strictly regulated. Access for non-governmental bodies would be subject to prior agreement from the brand owners.

Since verification rather than trust is an important aspect of tracking and tracing, and since every distribution chain is only as strong as it weakest link, all databases should be regularly subjected to external audits and any modifications of data and product recalls should be subject to very clear, transparent and stringent rules to ensure the integrity of the system.

04 Data carriers

The data carrier, usually including machine readable code, is a critical element of any system and enables simple and error free data exchanges. Data carriers used to uniquely identify (serializing) the different levels of packaging must:

- be easy to integrate into the production environments of the economic operators;
- be of a recognized global standard (GS1, AIM, ISO) to ensure quality & interoperability;
- be available in a range of different specifications to allow for the differing characteristics of the packaging levels;
- be implementable via as many different technologies as possible to ensure economic operators have the freedom to adapt the system to their particular operational circumstances.

ENSURING INTEROPERABILITY

Experience from a wide range of industries shows that successful deployment of track and trace systems depends on seamless interoperability among disparate information technology systems and internationally recognised technical standards that establish clear rules for capturing and sharing data. Systems of different economic operators and authorities involved along the legitimate supply chain should be able "to speak to each other", i.e. exchange data, irrespective of national borders.

Clearly defined standards are necessary to allow system interoperability, which enables different technology providers to develop their own TT&A solutions.

Policy makers should encourage technological architectures of a largely open nature, enabling interoperability across different technological platforms, geographies and industry sectors.

No single organisation or company could accept, deploy, manage and maintain an EU-wide TT&A system for all consumer goods. The complexity and size would just be too big to operate seamlessly, and the risk of the whole system becoming inaccessible or targeted by cybercriminals would be too high.

AGREEING MINIMAL TECHNICAL REQUIREMENTS

Coding system suppliers work with many global standards bodies such as ISO and most importantly for data carrier symbologies GS1.

Due to the complexity of the distribution chain and different packing levels of products, regulators or standard setting bodies will need to take into account that most solutions will require the use of multiple data carriers. Therefore, minimum technical requirements will need to be agreed upon, which will both accommodate this diversity of data carriers, and guarantee seamless input of information into databases.

To ensure interoperability between the different systems operated worldwide and across products, the choice of standards should be limited to three or four internationally recognised global standards with proven track records.

05 Reporting events

Track and trace systems track the movement of products forward through the different stages in the distribution and supply chain, and retrace the history of the products.

There is much discussion about the optimal frequency at which supply chain partners should report back to a track and trace system on events related to the products under their control (creation, packaging, movement of goods, changing of control).

While real-time or live reporting is often presented in theory as the optimal solution, ensuring that every product can be tracked in real time at every moment, the reality is often more complex than that.

The wholesale and distribution industry is a very important business sector in Europe, involving many players of different sizes, including a huge number of SMEs.

Forcing all partners in the supply chain to report in real time on any movement in goods would result in all of them, including the smallest family businesses, incurring great costs due to the necessary material investments in new IT systems. It would render more vulnerable the centralised databases, that would need to communicate non-stop with all other systems feeding into them.

Taking into account the objectives pursued by law enforcement, making track and trace information available to them within 24 hours is realistic and practically achievable without adding unnecessary costs to the system. In terms of impact on illicit trade, real-time reporting does not offer significant benefits to law enforcement when compared to daily reporting.

In the fight against illicit trade, track and trace systems are not generally used as a permanent inventory by law enforcement to see where a particular product is at any given time, but rather as a tool to establish a chain of custody and detect where products have been diverted from the legitimate distribution channels, or to establish whether they originate from a legitimate source.

Daily reporting also ensures a balanced data transmission volume, which is much easier to handle for the IT infrastructure supporting the system.

When it comes to the reporting language, standardisation can go a long way towards eliminating the complexity of having to use three different alphabets and 24 different languages in the EU alone.

06 Security Features

UNDERSTANDING DIFFERENT LAYERS OF SECURITY FEATURES

There are many options available when it comes to the authentication of a product. Relying on one solution is not recommended, with a layering approach favoured to provide more robust protection. Common layers of security used by economic operators to protect their manufactured goods include:

- Interactivity - This refers to a solution that employs a unique or serialized number (secure, unsecure, encrypted or not). Consumers can interact with the product and use the unique number to authenticate the goods, customs officials can use it to authenticate and establish the origin of the product.
- Overt authentication (visible). These types of solution are generally thought of as consumer verifiable and will include technologies such as; OVD (Optical Variable Devices), TEL (Tamper evident labels or tape) and colour shift technologies.
- Covert authentication (invisible unless a reading device is used). Covert solutions generally require trained user authentication as the general public should not be aware that a security feature has been deployed. A reading device is often necessary to detect the presence of a covert solution. Variants can include micro printing, UV-Visible/fluorescence marking, IR-Visible technology and taggant solutions.
- Forensic authentication (detection by analytical testing only). Detection of this type of solution will generally be required by a trained user via laboratory analytical methods such as spectroscopy. This includes packaging "fingerprinting", DNA markers or other additives.

Mass serialization is a rapidly growing trend within all manufactured goods as economic operators deploy practical solutions for their needs. However serializing a product only protects the packaging not the actual product. When used in conjunction with a tamper evident feature, it helps to further secure the integrity of the product.

ALLOWING TECHNOLOGICAL INNOVATION AND COMPETITION AMONG PROVIDERS

When it comes to fighting illicit trade, brand owners can now choose from a range of highly sophisticated devices and methods to protect their products thanks to developments in technology over the last 10 years. Regulators should define open specifications which allow the deployment of variable and layered solutions so that enforcement authorities and industry can stay one step ahead of counterfeiters.

Technical standards must ensure that there is no opportunity for misinterpretation of the result measured. Security features, although part of an open specification, must determine the authenticity of a product without interfering unduly with operational efficiencies or packaging functionality.

New technologies and methods to secure products are being developed continuously. It is therefore very important that legislators or initiatives of self-regulation do not limit the use of security features to those currently available. Authorities or regulators should provide an open and broad list of compliant security features from which brand owners can select the most suitable ones for their processes. To allow for technical innovation and competition, this list should be updated at regular

intervals and suppliers of security solutions should be allowed to submit their technology for certification and inclusion on the list.

Brand owners should be allowed to use the most appropriate solutions available and to determine the most effective means of authentication of products, provided that the systems respect agreed inter-operable standards.

This would create a level playing field amongst providers of security solutions, encourage competition and innovation and drive down prices, compared to a situation of quasi-monopoly for one or a limited number of solution providers, which would result from a closed list of available solutions, fixed in time.

CHECKING THE PRODUCT

The optimal approach to protect against counterfeiting includes several layers of security and authentication features to combine both overt and covert technologies, track and trace systems and tamper verification, thus making it as difficult as possible for counterfeiters and illicit trade to succeed. Furthermore, such layers should, wherever possible, be intrinsic to the item or packaging to ensure that the entire product is authenticated rather than the security feature alone.

No single solution or innovation should be considered in isolation and it is more effective to use layers or combinations of security that can be varied from time to time to avoid creating a counterfeiter's blueprint.

Security features which can readily be separated from the product or packaging and re-applied to counterfeit goods should be deprioritized in the layers chosen by operators and industry.

Coding systems of various technologies are well proven on all packaging applications found in manufacturing, however there is no "off-the-shelf" solution.

For fast moving consumer goods, several technologies have proven track records and several exciting new ones are in development. Printing or integrating code into the product through a different method ensures that the entire product is authenticated, but also technologies such as taggants, fingerprinting, micro texts, colour-shifting inks and charms offer cost-efficient solutions that can be easily integrated in high-speed production environments.

For regulated products, if legislation is implemented sensibly, there should be no requirement for sharing commercially sensitive information on features used. Such details should only be divulged on a need-to-know basis so as to reduce risk of details passing to counterfeiters.

EMPOWERING CONSUMERS VIA SMARTPHONE TECHNOLOGY

Consumers can be empowered to make their own judgement as to the authenticity of their goods and be able to control and check the properties and the value of what they buy, as counterfeit/authentic, stolen/legitimate, safe/dangerous, expired/usable, (in)appropriate for given dietary requirements.

TT&A technologies protect the supply chains in numerous industries and have been employed by brand owners, manufacturers and governments to combat smuggling of branded products and for quality control. These technologies enable supply chain partners to record, monitor and secure products as they move through the supply chain, and verify their authenticity.

Until a few years ago, most consumers never knew why products - from eggs to medication boxes - carry human and machine-readable codes. It is fair to assume their closest encounter with coding technology was usually checking the dates on the labels under "best before" and "use by" in the supermarket.

Things are starting to change for a combination of reasons, one of which is the inescapable presence of the internet in our increasingly networked world. Equally significant are the 2.6 billion smartphones connected to the internet — a figure that is predicted to top 6 billion by 2020. Together, these factors have so transformed the shopping experience that a recent survey by Planet Retail and GS1 UK found that 28% of shoppers would like to use their smartphone in-store to find what they're looking for, and 24% want to use a barcode scanner app to view more product information[5].

This is becoming increasingly possible thanks to the emergence of a number of new and affordable tools:

- Some brand owners and document issuers are open to sharing information explaining how to verify whether the product is original or counterfeit, which aspects of the packaging or product to look out for that are typically not well copied by counterfeiters, and so on. Unfortunately, this information is often buried in websites. Users are not aware of it and do not access it at the time where it matters, for example when buying the product. But this information becomes much easier to access if the user can access it by scanning a code on the product.

- A product that bears a unique identifier, such as a serialized 2D barcode, can be a powerful way to detect counterfeits and inform users about authenticity, even though it is easily copied. Full traceability in the supply chain is not required for this. What is required however are barcodes that can contain non-predictable data (either random or encrypted); the ability for users and consumers to scan the 2D barcode with a standard app and an active monitoring system. Let us take the example of a counterfeiter who inundates the market with 100,000 fake products, using one valid code from a genuine product to make his copies. Let us suppose that a mere 5% of products are scanned (a much higher percentage can be achieved if users are incentivised to scan or there is an education campaign). This means that the counterfeit code will be scanned an average of 5,000 times. With an active monitoring system, the presence of counterfeits will be quickly spotted and localized, and the brand owner can quickly inform consumers, "blacklist" the known counterfeits (by sending out an alert), and launch a product recall.

- One of the long recognised problems of first-level/overt solutions, such as hologram or colour-shifting inks, is that the average user typically has no idea about whether a security element should be present on the packaging, and even less so about how the security element should be verified. While there has been a quest for security features that are easy and intuitive to verify, the core issue remains. But this long-standing limitation of overt features is overcome by associating them with a unique identifier: when scanning a product, an animation can be shown indicating how to verify the security feature.

- The powerful image processing capabilities of mobile phones and their ever improving optical capabilities, can be used to authenticate secure graphics, digital watermarks, intrinsic features caused by natural randomness, as well as other optical effects. This, in effect, removes the responsibility of the authentication decision from users, as well as the inherent subjectivity of human decisions.

- Other sensory capabilities of mobile phones, such as their ability to read near-field communication (NFC) or other technologies that may emerge[6].

In summary, mobile phone-based product authentication solutions essentially make authentication more reliable and accessible to a

[5] Delighting the Modern Shopper, GS1 UK / Planet Retail, March 2015

[6] NFC is a set of communication protocols that enable communication between two electronic devices.

much wider group of people. Non-experts become far more effective in checking authenticity. The system becomes harder to circumvent for counterfeiters and allows for real-time feedback on authenticity, even in the absence of any security element. It could also increase the effectiveness of standard authentication solutions. And new image analysis-based methods allow for a standardized, objective authentication, reducing the responsibility of the operator in the authentication decision.

These developments give public authorities a real opportunity to ensure the general public and end users are aware and can sometimes even participate in either the process of authenticating or checking that a particular product has been authenticated.

As such, the consumer is no longer reduced to the role of innocent bystander or unwitting victim of illicit trade, but can also take responsibility for the purchase decisions made.

DETERMINING AUTHENTICITY

Brand owners and manufacturers are the first parties who have every interest in stopping the traffic of counterfeit versions of their own products. They are also ultimately the ones who should be in a position to sue the counterfeiters and their accomplices along the supply chain for lost income and reputation damage to their brands.

For this reason they often make big investments in securing their own supply chains, stopping diversions of their products from the legitimate distribution chain and limiting the possibility of counterfeit products being substituted for their own genuine products.

All other participants in the supply chain also have a responsibility to collaborate and ensure that their part in the overall chain is secured by accurately logging and transmitting all necessary data on the movement of the products.

The brand owner / manufacturer should determine whether seized products are genuine or counterfeit in collaboration with enforcement authorities. This will ensure reliable measurement using accurate verification techniques. It will also enable the company whose product is counterfeited to implement corrective security measures.

In certain, more regulated sectors, where legitimate products are sometimes also diverted from the regular distribution chain in order to avoid excise duties or taxes, law enforcement and public authorities can put in place additional verifications and independent controls to safeguard their interests.

07 Implementation cost

Firstly, it is very important to refer back to the principle that any track and trace system should be devised to avoid unnecessary complexity and costs, and to account for the value of the products it protect.

Since all parties involved in the distribution chain have a vested interest in securing it, it also seems reasonable that there is equitable burden sharing between manufacturers, brand owners, wholesalers, distributors and public authorities. Once a system is agreed upon between the different parties, every party should bear its own part of the burden for implementing it and the industry will need to be persuaded that this investment can also be made in their own best interest.

Where TT&A applications are made compulsory by governmental directives and regulations, particular attention should be paid to the fact that initial investments should be viable for every company and operator in a given industry and market sector in order not to discriminate between companies.

For that reason, the selection of relevant technologies to perform TT&A should be left to the economic operators of the supply chain, in compliance with defined standards. Identification devices may differ along the supply chain. Operators should be in the position to select the most suitable ones for their processes.

This will also encourage competition between solution and equipment providers and avoid monopolies, which have a tendency to drive up costs and inhibit innovation.

Open specification allowing commercial competition amongst the supply base for such technologies will improve the cost-benefit ratio. The cost of application should be carried by industry (TT&A will pay for itself in reality), but measurement and compliance should be at the cost of regulatory jurisdiction.

A critical factor in determining whether a system is cost-effective is defining how any deployed solution impacts existing manufacturing operations. A digital in-line system where the data carrier is printed directly onto the packaging is at least 10 times more efficient than a traditional stamp application solution (based on the recognized fact that applying stamps reduces overall production effectiveness, with an average of 2% of products rejected by the equipment due to erroneous application).

08 Conclusions and recommendations

Public authorities and regulators have a critical role to play in supporting the development of relevant technological architectures to guarantee interoperability across different technological platforms, geographies and industry sectors.

The selection of relevant technologies for TT&A should be left to the economic operators of the supply chain, in compliance with technical standards agreed by public authorities or international standard setting bodies.

The purpose of T&T systems is to monitor product movements and changes in ownership throughout the supply chain. This information can only be provided by economic operators handling distribution and administrative accounting procedures in warehouses.

T&T systems should not duplicate, but complement and be compatible with, established systems and procedures. Moreover, a business-friendly system would provide an opportunity to leverage data mining and insights on production, distribution and product life-cycle.

"Unique identifiers" are an enabling tool rather than the objective of a T&T system. Meanwhile data carriers become crucial in the context of mass production of goods requiring high speed manufacture, to avoid disruption in the supply chain.

A clear distinction should be made between system operation and independent control.
The identification and operation of the most appropriate system should remain with manufacturers and other economic operators

involved. Beyond the internal checks carried out by the economic operator, independent third-party checks should be conducted by public authorities or by agreed bodies authorised by public authorities.

Given the commercial sensitivity and the liability in case of technical failures, stored data should be considered confidential and owned by the manufacturer or brand owner where data is stored locally. Meanwhile, data should be accessible to certified third-parties such as auditors, law enforcement and public authorities only under strict conditions.

Any selected standard for track and trace or authentication features should be an open specification that allows systems that use a range of familiar and proven technology platforms and solutions. Reliance on one or a small selection of solution suppliers will increase the risk of delays in deploying any selected TT&A system, and its effectiveness.

Avoidance of redundant complexity and costs should be built into the design of all track and trace systems from system inception to system management. Such systems must take into account the value of the products they protect, and safeguard a level playing field for operators to ensure the investments required in the system do not act as a discriminatory barrier for SMEs.

The constant development of smartphone technology should be leveraged by brand owners to better engage and empower consumers in the fight against illicit trade and counterfeiting.

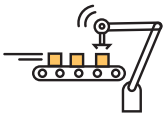
For regulated products and processes, non-compliance by economic operators should be clearly sanctioned and associated with proportionate penalties as a deterrent against the non-implementation of the statutory requirements in TT&A.

TOWARDS OPTIMAL TRACKING, TRACING & AUTHENTICATION SYSTEMS TO COMBAT ILLICIT TRADE AND COUNTERFEITING

1 DETERMINING RESPONSIBILITY & ACCOUNTABILITY

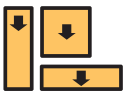
Public authorities define open specifications which determine the purpose and function of the TT&A solution from a public policy perspective.

Manufacturers and supply chain operators select the appropriate technologies for their TT&A standards and production facilities based on:

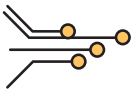


Ease of integration into production

Recognized global standards to ensure quality & interoperability



Available in different specifications for different levels of packaging



Choice of technology to adapt system to particular operations

Manufacturers perform the first level of any tracking & tracing system

Supply chain participants have the responsibility to collaborate and ensure accurate logging and transmission of all required T&T data

2 DATA FLOW, STORAGE & REPORTING

Digital Track & Trace systems delivers data tracking the movement of products through the supply chain

Policy makers define what data needs to be collected in a database

Individual manufacturers operate the database for their own products, keeping data secure and confidential

Interoperable standards and solutions allow different actors in the supply chain to perform the necessary checks

Daily reporting by supply chain partners to a T&T system on the movement of goods under their control

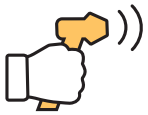
Data relevant to law enforcement & national authorities can be transferred to external database in a strictly regulated manner

Independent operators & public authorities can audit the database

3 AUTHENTICATION

Leveraging technological innovation to facilitate product authentication from the manufacturer to the consumer

A mix of layers of security features is needed to secure the integrity of a product



Open standard TT&A features compatible and interoperable with a wide range of proven technology platforms to check and identify products

Technological innovation and competition among providers through open specifications ensures staying ahead of counterfeiters

Products can be verified at each stage on the distribution chain

Deployment of constantly evolving smartphone technology empowers consumers to determine the authenticity of products

Manufacturers together with law enforcement authorities determine if a seized product is genuine or counterfeit

COALITION
AGAINST ILLICIT TRADE

For further information on the Coalition Against Illicit Trade:
http://www.coalitionagainstillicittrade.org/

If you wish to support CAIT or participate to future activities, please contact us at:
enquiries@coalitionagainstillicittrade.org