Implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products

Final Report

Service Contract N° 2015 71 05

everis
April 2018

Public Health

EUROPEAN COMMISSION

Consumers, Health, Agriculture and Food Executive Agency
Health Unit

Directorate-General for Health and Food Safety
Directorate B-Health systems, medical products and innovation
Unit B2- Health in all policies, global health, tobacco control

E-mail: *CHAFEA-HP-TENDER@ec.europa.eu*

SANTE-B2-Tobacco-Control@ec.europa.eu

European Commission
B-1049 Brussels

Implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products

Final Report

Service Contract N° 2015 71 05

Consumers, Health, Agriculture and Food Executive Agency
Health Programme

This report was produced under the health Programme (2014-2020) in the frame of a specific contract with the Consumers, health, Agriculture and Food Executive Agency (Chafea) acting under the mandate of the European Commission. The content of this report represents the views of the contractor and is its sole responsibility; it can in no way be taken to reflect the views of the European Commission and/or Chafea or any other body of the European Union. The European Commission and/or Chafea do not guarantee the accuracy of the data included in this report, nor do they accept responsibility for any use made by third parties thereof.

More information on the European Union is available on the Internet (http://europa.eu).

Luxembourg: Publications Office of the European Union, 2018

PDF	ISBN 978-92-9200-770-6	doi:10.2818/453932

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

0. INTRODUCTION

The following document serves as the Final Report to the European Commission´s Consumers, Health, Food and Agriculture Executive Agency (Chafea) in response to the request for service Chafea/2015/health/40 for the implementation of Framework Contract FWC DIGIT/R2/PO/2013/004 ABC III Lot 2, concerning the implementation analysis regarding the technical specifications and other key elements for a future EU system for traceability and security features in the field of tobacco products.

The present document is the main report of the study carried out, and is complemented by:

- Annex I – Evaluation of Policy Options
- Annex II – Technical Specifications of the Tracking and Tracing System and the Security Features
- Annex III – Model Contract

All these documents are made public, and can be requested under the following publication numbers:

Volume	Catalogue number	ISBN	DOI
Annex I – Evaluation of Policy Options	EB-02-17-896-EN-N	978-92-9200-874-1	10.2818/628162
Annex II – Technical Specifications of the Tracking and Tracing System and the Security Features	EB-02-17-897-EN-N	978-92-9200-875-8	10.2818/343517
Annex III – Model Contract	EB-02-17-898-EN-N	978-92-9200-876-5	10.2818/751591

1. Abstract

The Implementation Study aimed at assisting the European Commission in defining the Implementing and Delegated Acts to develop and implement a tracking and tracing system for tobacco products at unit packet level, in line with Articles 15 and 16 of the TPD.

To achieve these goals, the Implementation Study was divided into four work packages, and further separated into ten tasks that conclude with the preparation of this Final Report. The Final Report itself is divided into three main parts: general concept of the Tracking and Tracing System, technical specifications of the Tracking and Tracing System, and technical specifications of the security features.

The **general concept of the Tracking and Tracing System** aims to provide a clear view of the proposed Tracking and Tracing System and is divided in three sections:

- The **project charter** includes the fundamental information used to establish the basis of the future Tracking and Tracing System, such as its legal basis, success criteria, scope, assumptions, constraints, and a roadmap.
- The **high level solution design** presents a summary of the definition and characterisation of all policy options under evaluation. It also selects the options in each decision point based on the evaluation criteria.
- The **cost-benefit analysis** gives a summary of an extensive analysis carried out in Interim Report II, which describes the benefits associated with the effective implementation of the proposed measures, together with the costs of the new Tracking and Tracing System, through the entire tobacco supply chain.

The **technical specifications of the Tracking and Tracing System** provides the technical specifications of the elements required for the successful implementation of the Tracking and Tracing System:

- **Supply chain elements**: includes the description of the unique identifier, the recommended data carriers, and the anti-tampering system;
- **IT artefacts**, whose elements are: system architecture (Primary and Surveillance Data Storage, Repository Router, ID Issuer and the optional Temporary Buffer to report events from the facilities), data dictionary and messaging.

The **technical specifications of the security features** provides a description of the activities related to the integration of the security features on tobacco products. These activities fall into different categories, according to:

- The use of a tax stamp as a security feature;
- The integration of the security feature directly onto the tobacco product;
- The integration of the security feature as a label.

2. Executive Summary

The Implementation Study aimed at assisting the European Commission in defining the Implementing and Delegated Acts to:

- Develop and implement an EU Tracking and Tracing System for tobacco products at unit packet level, in line with Article 15 of the Tobacco Products Directive (TPD);
- Develop and implement a system that ensures that all unit packets of tobacco products, which are placed on the EU market, carry a tamper-proof security feature composed of visible and invisible elements, in line with Article 16 of the TPD.

To achieve these goals, the Implementation Study was divided into four Work Packages, as presented below.

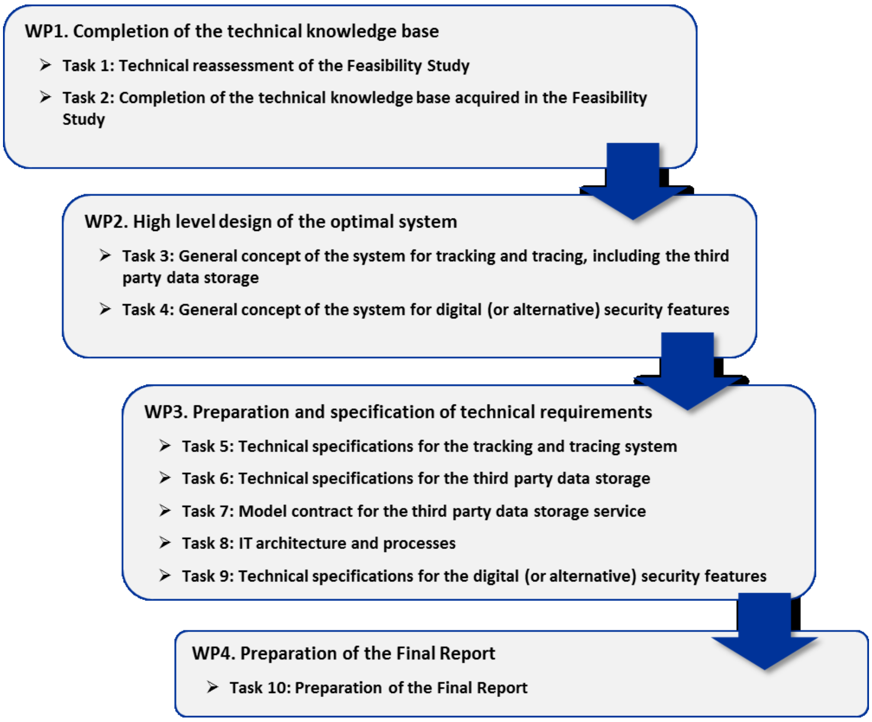


Figure 1: General overview of the Implementation Study Work Packages

2.1. General concept of the System

This section contains fundamental information used to present the basis of the future Tracking and Tracing System.

High level solution design

The high level solution design draws on the knowledge gathered during the implementation of Work Package 2. The findings of this Work Package in relation to the assessment of the policy options were used to develop the high level optimal system presented in the table below.

Tracking and tracing				Security features
Who?	**Where?**	**How?**	**When?**	**How?**
(A) Governance model	**(B) Data storage model**	**(C) Allowed data carriers**	**(D) Allowed delays in reporting events**	**(S) Method of adding a security feature**
(A1) Industry operated solution	(B1) Centralised model	**(C1)** System with a single data carrier for all identification levels	**(D1) Near real-time reports**	**(S1)** Affixing
(A2) Third party operated solution	**(B2)** Decentralised model per manufacturer/ importer	(C2) System with a single data carrier per identification level and optional data carriers for aggregation packaging levels	**(D2)** One day delay reports	**(S2)** Printing or integrating through a different method
(A3) Mixed solution (industry and third party)	**(B3)** Decentralised model per Member State	**(C3)** System with a limited variety of data carriers for all identification levels	**(D3)** One-week delay reports	**(S3) Mixed solution**
-	**(B4) Combined model: centralised for surveillance and decentralised for recording per manufacturer/ importer**	**(C4) System with limited variety of data carriers for all identification levels and optional data carriers for aggregation packaging levels**	-	-
-	-	**(C5)** Free system allowing any existing approved data carrier	-	-

Table 1: Optimal system based on the assessment of the policy options

Cost-benefit analysis

Illicit tobacco trade has been estimated to account for 11.26% (see Annex I – Chapter 2: *Assessment for the calculation of the cost-benefit analysis*) of the total consumption of tobacco products in the European Union. Implementing effective measures to control and fight against this illicit trade will contribute to reducing tobacco consumption, and the effect of this reduction is expected to be threefold (Reed, 2010):

- Some smokers will smoke less;
- Others will stop smoking altogether; and
- Smoking take-up will decline, increasing the number of non-smokers.

The benefits associated with the effective implementation of the proposed measures are classified by their nature, economic benefits, and social and environmental benefits. Interim Report II performs an extensive analysis that collects and calculates these benefits by studying concepts and figures such as price elasticity, consumption and socio-economic figures by Member State.

- **Economic benefits**, defined as the net income generated as the result of the implementation of the proposed measures and divided in two sub-categories:
    - Revenues from an increase in legal sales

- Rise in tax collection resulting from an increase in legal sales.
- Profits from increased sales for legal economic operators.

- Other economic benefits
  - Reduction in costs associated to public health savings.
  - Benefits derived from an increase in productivity.

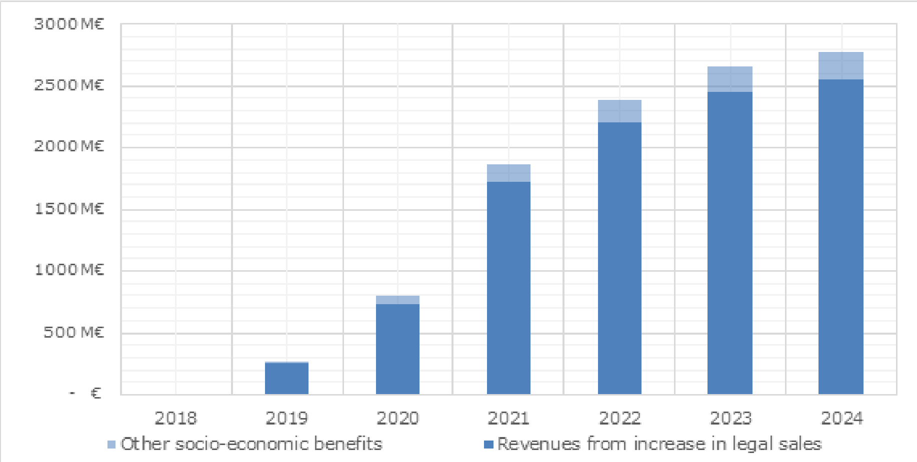


Figure 2: Breakdown of the economic benefits (million €) – Interim Report II

- **Social and environmental benefits**. The reduction of smoking produces several social and environmental benefits to society. The main impact in this regard is the improvement of public health.
  - People who reduce or quit smoking
    - A percentage of illicit tobacco purchasers will decide to reduce their consumption, or even quit smoking (Transcrime, Joint Research Centre on Transnational Crime, 2015)
    - 712,000 persons will reduce or quit smoking[1].
  - Reduction of costs associated with premature mortality due to smoking
    - People who do not smoke or reduce their consumption of tobacco products until eventually quitting smoking are healthier and live significantly longer (Peto, Lopez, Boreham, & Thun, 2012).
    - The decrease in the number or life years lost will reach an estimated total of 60,274[2] in the European Union.
  - Other social and environmental benefits
    - Reduction of costs associated with fires caused by smokers' materials.

[1] See Table 16: Summary of the social benefits I in section 4.3.1.2 Social and environmental benefits
[2] See Table 17: Summary of the social benefits II in section 4.3.1.2 Social and environmental benefits

- Improvements in the distribution chain, by reducing associated risks and enhancing visibility across stages (Aung, 2013).
- Reduction in financing of criminal groups (US Department of State, 2015).

In order to analyse the full cost of the new Tracking and Tracing System within the tobacco supply chain, the total cost has been divided into five parts corresponding with the five proposed policy options.

A. **Governance model**, which ensures the required level of system integrity by the allocation of various responsibilities and functions to the operators involved in the supply chain, in compliance with the requirements of the FCTC Protocol and the TPD

B. **Data storage model**, which aims to store all relevant data reported by the economic operators, assure its integrity, and make it accessible to the competent authorities for surveillance purposes.

C. **Allowed data carriers**, which intends to describe the allowed set of data carriers that will contain the unique identifiers.

D. **Allowed delays**, which ensures that traceability and trade data are transmitted to and recorded in the Tracking and Tracing System.

S. **Method of adding a security feature**, which focuses on how to add the security features to unit packets of tobacco products.

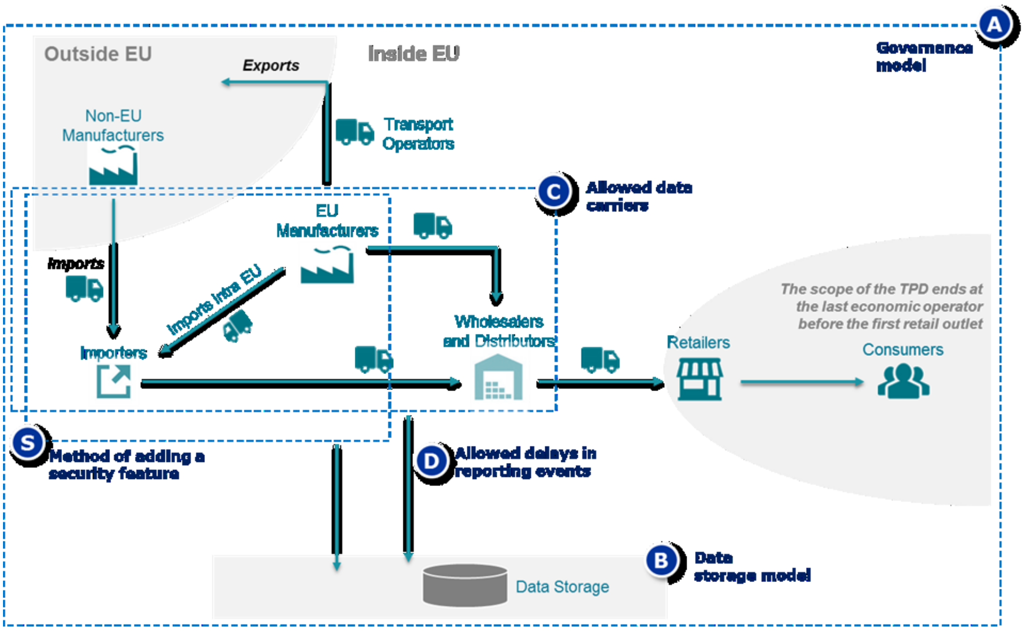


Figure 3: Tracking and Tracing System schema

The costs are distinguished between CAPEX (capital expenditures) and OPEX (operational expenditures) and they are depreciated over a six year time period. Additionally, the CAPEX corresponding to the implementation of the System for cigarettes and RYO is estimated for 2018, while the CAPEX for the implementation of the System for other tobacco products is forecast for 2023. The OPEX starts as of May 2019 for tobacco and RYO and May 2024 for other tobacco products.

The detailed analysis of the cost calculation is presented in Interim Report II, where costs such as data carrier generation, printing, and verifying and scanning equipment, as well as the costs related to software, hardware, communications and system auditing are identified. The following table summarises the annualised costs split by typology and policy option.

	2018	2019	2020	2021	2022	2023	2024
CAPEX - Governance model	92.56	-	-	-	-	3.78	-
CAPEX - Data storage model	18.26	-	-	-	-	0.75	-
CAPEX - Allowed data carriers	160.98	-	-	-	-	6.59	-
CAPEX - Allowed delays in reporting events	37.45	-	-	-	-	1.53	-
CAPEX - Method of adding a security feature	-	-	-	-	-	-	-
CAPEX - TOTAL	309.26	-	-	-	-	12.65	-
OPEX - Governance model	-	17.25	25.88	25.88	25.88	25.88	26.58
OPEX - Data storage model	-	4.66	7.00	7.00	7.00	7.00	7.19
OPEX - Allowed data carriers	-	6.18	9.28	9.28	9.28	9.28	9.53
OPEX - Allowed delays in reporting events	-	27.00	40.51	40.51	40.51	40.51	41.61
OPEX - Method of adding a security feature	-	9.53	14.30	14.30	14.30	14.30	14.69
OPEX - TOTAL	-	64.64[3]	96.97	96.97	96.97	96.97	99.61

Table 2: Detailed CAPEX and OPEX (Millions of euros) - Interim Report II

2.2. Technical specifications for the Tracking and Tracing System

The Tracking and Tracing System provides information about the products' progress through the supply chain by recording the required information in the successive stages of the physical flow. It can be divided into three major conceptual domain groups, namely:

- **Supply chain**: the domain where merchandise is traded;
- **IT**: the domain that interacts with information, further divided into:
  - **UI generation**: the domain where the unique identifier is generated.
  - **Data storage**: the domain where the data is stored.
- **Surveillance**: the domain where competent authorities and auditors access data.

An overview of the Tracking and Tracing System is depicted in the diagram below:

[3] The OPEX for 2019 are influenced by the fact that the measure becomes effective in May of that year.

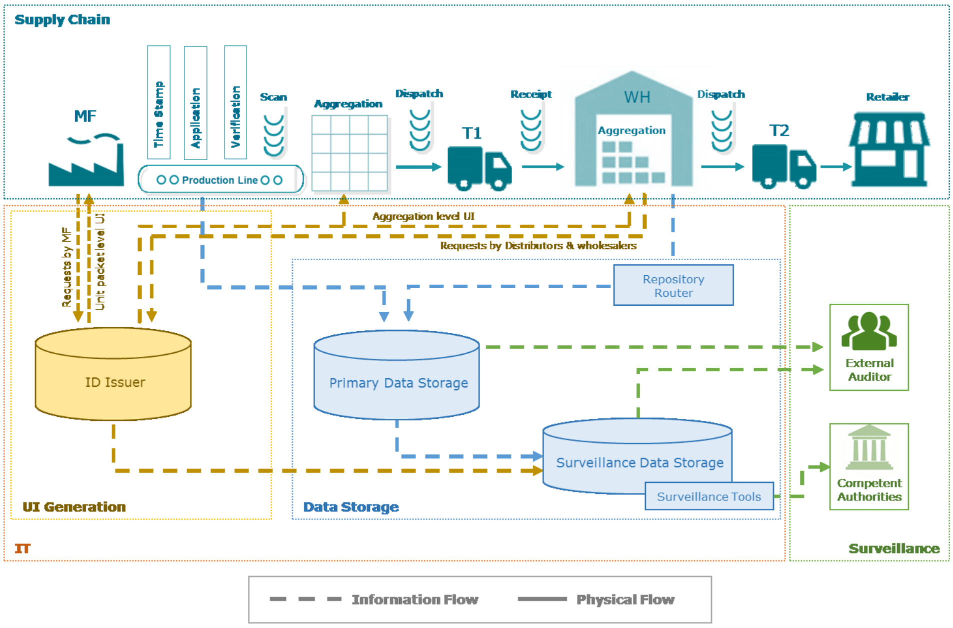


Figure 4: System overview diagram

This report provides a conceptual design of the elements belonging to Supply Chain and IT domains, which were firstly developed in Work Package 3, are explained below.

Supply chain elements

- ***Unique identifier (at unit packet level/ aggregation packaging level)***

  This report evaluates the composition of the unique identifiers at unit packet and aggregation packaging levels. It includes all the information requested by the TPD, while considering two inherent challenges to the supply chain implementation:

  - The excessive length of the unique identifier as a negative factor in printing performance;
  - The access to readable information for competent authorities.

  Addressing these two challenges, combined with the use of lookup tables, results in a significant reduction of code length. A summary of the code composition is presented in the tables below.

  <u>Composition of the unique identifier at unit packet level</u>

Element ID	Information requested	TPD Reference	Code example	Length estimation
UID_1	**ID Issuer identification**		A3	2
UID_2	**Serial number**		AAE5F46G7H	10
UID_3	**Place** of manufacture	Art 15(2)(a)	A1B2C3D4L2M3N4	14
	Manufacturing **facility**	Art 15(2)(b)		
	Machine used to manufacture the tobacco	Art 15(2)(c)		

Element ID	Information requested	TPD Reference	Code example	Length estimation
	products			
	Product description	Art 15(2)(e)		
	Intended **market** of retail sale	Art 15(2)(f)		
	Intended shipment **route**	Art 15(2)(g)		
	Where applicable, the **importer** into the EU	Art 15(2)(h)		
UID_4	**Date** of manufacture	Art 15(2)(a)	21043013	8
	Production shift or **time** of manufacture	Art 15(2)(d)		
Total				**34**

Table 3: Structure of the unique identifier at unit packet level

Composition of the unique identifier at aggregation packaging level

Element ID	Information provided	Code example	Length estimation
UID_1	**ID Issuer identifier**	A3	2
UID_2	**Serial number**	T03K55E322	10
UID_3	**Location** of the aggregation activities	A1B2	4
UID_4	**Date** of the aggregation activities	21043013	8
Total			**24**

Table 4: Structure of the unique identifier at aggregation packaging level

- ***Data carrier (at unit packet level/aggregation packaging level)***

  The selection of data carriers responds to the need to contain the unique identifier while limiting the impact on manufacturing and distribution operations. Therefore, an extensive review of data carrier processes and operations has been made to outline the key drivers influencing their selection. The results of this review are summarised below and presented in further detail in the chapters that follow.

  - At unit packet level:
    - Production speed (high-speed vs low/medium-speed production lines)
    - type of tobacco products (cigarettes vs other tobacco products than cigarettes).

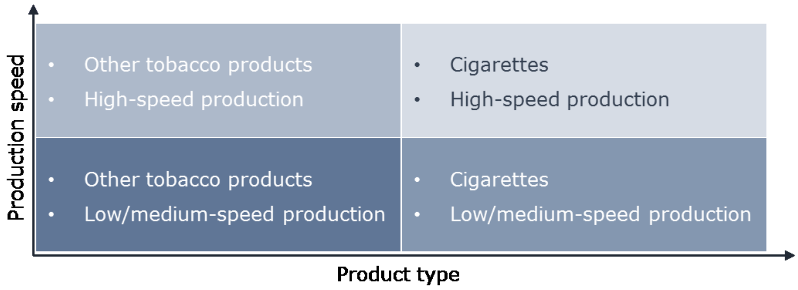


Figure 5: Product type vs production speed matrix

- At aggregation packaging level: Aggregation level

Figure 6: Levels of aggregation of tobacco products

The most adequate data carriers are selected by means of an analysis influenced by the following evaluation parameters:

- Technical feasibility
- Operational requirements
- Burden on stakeholders

A summary of this selection is presented in the tables below.

Recommended data carriers at unit packet level

Data Carrier	Characteristics	Example
Data matrix	• Can be printed by multiple technologies either directly onto the package or on a label to later be affixed. • Currently used in the marking of tobacco products other than cigarettes.	
DotCode	• Can be printed in high-speed production lines through continuous ink jet or laser printing technologies. • Currently used at unit packet level by several tobacco manufacturers.	
QR	• Can be printed by multiple technologies either directly on the package or on a label to later be affixed. • It is one of the most used data carriers worldwide and compatible with multiple scanning solutions.	

Recommended data carriers at aggregation packaging level

Data Carrier	Characteristics	Example

Data Carrier	Characteristics	Example
Data matrix	• Can be printed by multiple technologies, either directly on the package or on a label to later be affixed. • Currently used in the marking of aggregation packaging of tobacco products.	
Code 128	• Widely used in logistics operations and can be read by laser scanners. • Currently used in the marking of aggregation packaging of tobacco products.	
QR	• Can be printed by multiple technologies either directly on the package or on a label to later be affixed. • Is one of the most widely used data carriers worldwide and is compatible with multiple scanning solutions.	

- ***Anti-tampering system***

The anti-tampering solution protects the process of verifying unique identifiers following their applications, whilst maintaining the flexibility of operation and maximising the potential of reducing illicit trade. Since there is a wide variety of manufacturing lines and based on the analyses made, this report proposes three anti-tampering solutions to better meet manufacturer needs.

Automated manufacturing lines

Option 1.1 – Image production controlling

This option proposes the use of image production controlling as an anti-tampering solution in the manufacturing lines of tobacco products. This solution is based on ensuring the marking of unit packets by comparing the unit packet production with the number of unique identifiers reported to the Primary Data Storage. Moreover, additional applications can be built from the data recorded, establishing real-time alerts or providing valuable insight to further audits or inspections.

Option 1.2 – CCTV video surveillance with production control

The second option is a system combining the security component of CCTV video surveillance and the counting of manufacturing flow in order to detect potential deviations and unauthorised tampering attempts by comparing production rate with the number of unique identifiers sent to the Primary Data Storage.

Non-automated manufacturing lines

Option 2.1 – CCTV video surveillance in non-automated manufacturing lines

This option is a system based on CCTV video surveillance that keeps record of the activities near the verification system. This solution is specially envisioned for manufacturing facilities with a low production rate, where production is not fully automated and uses a variety of manual processes.

IT Artefacts

- ***System architecture***

This section describes the individual systems or solutions that compose the Tracking and Tracing System, and how these systems interact with each other and with external systems. These individual systems are:

- Primary Data Storage;
- Surveillance Data Storage; and
- ID Issuer solution.

Two major architectural decisions have been made: a) establishing a central component (i.e. Repository Router), where the distributors and wholesalers seamlessly report all relevant data; and b) using a canonical data model, in order to exchange tracking and tracing data with the competent authorities and auditors (see details in section 3.1.3 of "*Annex II: Technical Specifications of the Tracking and Tracing System*").

Interim Report III identifies the interfaces that will carry out the interactions of these systems in a secure and standardised way. It also provides a detailed description of the requirements of each main architecture component of the Tracking and Tracing System (using the RUP@EC methodology). Namely:

- **Primary Data Storage solution**. This solution hosts data exclusively related to a specific manufacturer or importer. It is envisaged that different Primary Data Storage solutions may be established.
- **Surveillance Data Storage solution**. This is a global copy of the tracking and tracing data, which will facilitate enforcement activities. This central solution also includes a message router (i.e. Repository Router).
- **Repository Router**. This component is responsible for routing the messages transmitted from the distributors and wholesalers to the corresponding Primary Data Storage that receives them.
- **ID Issuer solution**. This solution, which is established at a national level, is responsible for generating unique serial numbers, at unit packet or aggregation packaging level. Moreover, it offers registration services to the economic operators, which enables the population of lookup data needed for the unique identifier serialisation.
- **Temporary Buffer**. This is an optional on-site component, which is established on a voluntary basis by the economic operators at a facility level and reports events to the Tracking and Tracing System. It is recommended because it decouples the manufacturing and distribution activities from the transmission of events and also mediates communication between data sources of the economic operators' proprietary solutions and the Tracking and Tracing System.

It is important to note that these components shall be able to operate on a very large scale in highly critical environments. The requirements specification in this report covers different topics, namely: expected functionality, qualities (e.g. performance, reliability, maintainability, etc.), security, design constraints, applicable standards, and interfaces.

- ***Data dictionary and messaging***

  The data dictionary is the main deliverable of the work stream on the logical data structure of the System, providing organised visibility and understanding of the data elements and their relationships. The section explains each group of data and their conceptualised usages. The resulting data dictionary is converted into a canonical data model in order to give competent authorities standardised access to the Tracking and Tracing System data.

  The messaging provides the technical definition, which also includes an extensibility mechanism, to allow the exchange of data with the individual components of the Tracking and Tracing System, the data sources, and the data consumers. The definition provides different message structures driven by each data exchange requirement.

2.3. Technical specifications for the security features

This report provides a description of the activities related to the integration of the security features on tobacco products. These activities fall into several categories, according to:

- The use of tax stamp as a security feature;
- The integration of the security feature directly on the tobacco product;
- The integration of the security feature as a label.

The main actors involved in the related processes are the tobacco manufacturers and importers of tobacco products.

Article 16 of the TPD requires all unit packets of tobacco products placed on the market to carry a tamper-proof and irremovable security feature, composed of visible and invisible elements, as a method of fighting illicit trade.

In order to maximise the proposed Tracking and Tracing System and help fight the illicit trade of tobacco products, different considerations related to security feature requirements are highlighted in this report. These include the security of production, application methods, exchange of information with competent authorities, and confidentiality, as well as the selection of security features in order to provide guidelines to all entities involved in the process.

In addition, security feature counterfeiting is a widespread problem that affects public authorities, manufacturers, distributors and solution providers. Therefore, this report identifies the different risks associated with security features; namely those related to counterfeiting and the security of production, transport and storage of security features.

In order to ensure the integrity of the security features, it is important to remove security elements once they have been compromised, and regularly integrate new hidden security features. It is recommended that the security features and their specific elements be reviewed every three to five years (at minimum every five years).

3. Background of the Report

3.1. Context and objectives

The objective of the Implementation Study was to support the European Commission in preparing the Implementing and Delegated Acts foreseen under Articles 15 and 16 of the TPD. The Implementing and Delegated Acts will effectively set the rules for the establishment and operation of EU systems of tobacco traceability and security features. These systems will be applicable to cigarettes and roll-your-own tobacco products as of 20 May 2019 and to other tobacco products as of 20 May 2024.

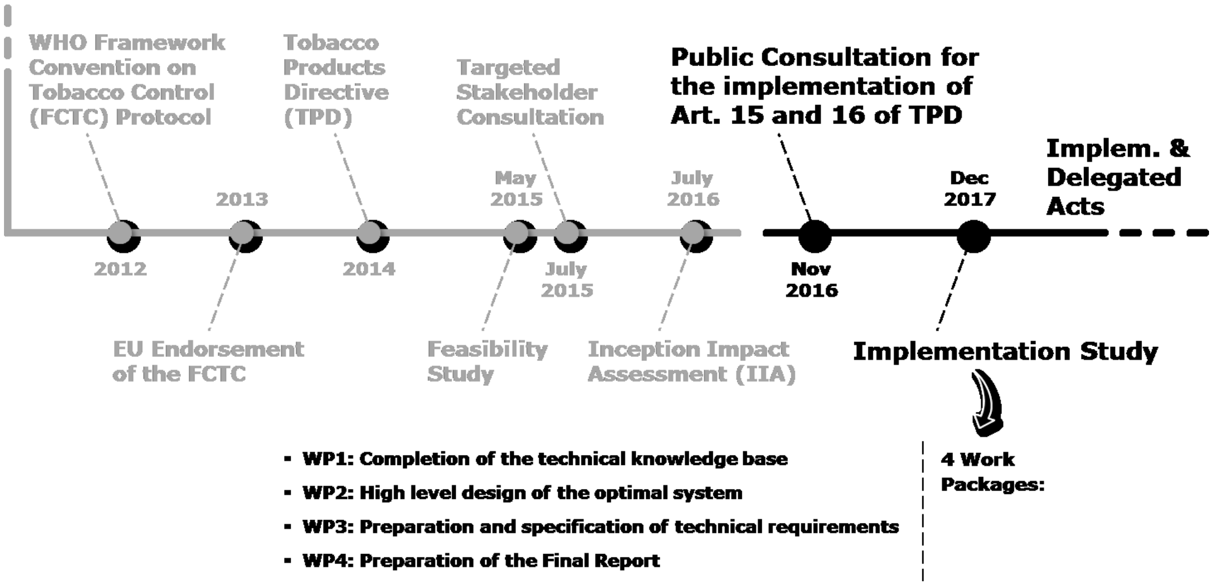


Figure 7: Overview of the planning

The Implementation Study took past initiatives into consideration as well as those still in progress.

As shown in the planning above, the following initiatives have been taken into account and assessed for the purposes of developing this report:

- The Tobacco Products Directive (TPD)
- Feasibility Study
- Targeted Stakeholders Consultation
- Inception Impact Assessment
- Public Consultation for the Implementation of Art.15 and 16 of TPD

3.1.1. The Tobacco Products Directive (TPD) and the Framework Convention for Tobacco Control Protocol (FCTC Protocol).

The overall objective of the TPD is to provide a framework for laws, regulations and administrative provisions in the Member States concerning the manufacture, presentation and sale of tobacco and related products. It includes traceability and security features, which are intended to increase security and control throughout the entire tobacco supply chain. The TPD facilitates the smooth functioning of the internal market for tobacco and tobacco related products, using as its basis a high level of protection of human health, especially for young people. In this regard, it addresses the obligations of the European Union (EU) under the Framework Convention for Tobacco Control (FCTC).

The Protocol to Eliminate Illicit Trade in Tobacco Products, the first Protocol to the FCTC, was adopted on 12 November 2012. In June 2016, the European Union formally ratified the FCTC Protocol. In so doing,, it confirmed its intention to implement in full the provisions of the Protocol that fall into the categories and areas of Union competence.

According to the declaration submitted by the European Union pursuant to article 44 of the FCTC Protocol, the EU has exclusive competence to act with respect to the matters covered by the FCTC Protocol that fall under the scope of the common commercial policy of the EU (Article 207 TFEU). In addition, the EU has exclusive competence to act with regard to matters covered by the FCTC protocol that fall under the scope of customs cooperation (Article 33 TFEU), approximation of laws in the internal market (Articles 113 and 114 TFEU), judicial cooperation in criminal matters (Article 82 TFEU) and definition of criminal offences (Article 83 TFEU), only insofar as the provisions of a Union act establish common rules that may be affected or altered in scope by provisions of the FCTC protocol.

Articles 15 and 16 of the TPD aim at fighting the illicit trade of tobacco products and thus, from a public health perspective, contribute to reducing the low cost supplies of illegal tobacco products that increase the uptake and general prevalence of smoking. Article 15 of the TPD requires tobacco products to be tracked and traced. In order to achieve this, all unit packets of tobacco products manufactured in or imported into the European Union must be marked with a unique identifier (containing defined data elements). Furthermore, their movements must be recorded throughout the supply chain (up to the last level before the first retail outlet). In addition to tracking and tracing, Article 16 requires that all unit packets of tobacco products that are placed on the EU market carry a tamper-proof security feature composed of both visible and invisible elements.

The implementation of the traceability system under Article 15 of the TPD will be the means by which the EU will implement Article 8 of the FCTC Protocol, which provides for the establishment of a global tracking and tracing regime consisting of national and/or regional systems. It is essential to bear in mind that Article 8 requires each tracking and tracing system to be controlled by the Party who establishes it. In all cases, therefore, overall control of the traceability system should be with the authorities.

3.1.2. Feasibility Study

The European Commission's Consumers, Health and Food Executive Agency (CHAFEA) commissioned a feasibility study (Feasibility Study, 2015) concerning the provision of an analysis and feasibility assessment regarding EU systems for tracking and tracing tobacco products and for security features (hereinafter "the Feasibility Study").

The Feasibility Study is a thorough and extensive review with a high level of detail encompassing the main components of a future EU Tracking and Tracing System. The basis of the study was the following:

- A market assessment and mapping of existing traceability and security feature solutions suitable for tobacco products;

- Development of a comprehensive problem statement, taking into consideration the regulatory reference points (e.g. TPD), and the requirements of multiple stakeholders;
- Possible options for tracking and tracing as well as security features;
- Benchmarking of tracking and tracing systems currently in operation.

3.1.3. Targeted Stakeholder Consultation

The objective of the Targeted Stakeholder Consultation (European Commision - Targeted stakeholder consultation TPD, 2015) was to provide stakeholders with the opportunity to comment on the findings of the Feasibility Study.

The targeted stakeholders were manufacturers and importers of finished tobacco products, wholesalers and distributors of finished tobacco products, providers of solutions for operating traceability and security feature systems, and governmental and non-governmental organisations active in the area of tobacco control and the fight against illicit trade. They were advised to review the Feasibility Study before responding to this consultation, which was made available online from 7 May 2015 to 31 July 2015.

The Targeted Stakeholder Consultation received 109 responses. The contributions reflect the opinions of both large[4] and small tobacco manufacturers in the EU, as well as manufacturers of cigars and other tobacco products, international supply chain managers and local distributors, large scale service providers and niche market players, NGOs active in the fight against illicit trade in tobacco products and sectorial associations, governmental organisations, and others – essentially those parties affected by changes in tobacco policy. Both the large turnout and the detailed nature of the comments received highlight how high the stakes in this area are.

The Targeted Stakeholder Consultation gathered a great deal of input regarding stakeholder concerns about the options and solutions proposed in the Feasibility Study. These stakeholders also contributed some recommendations and proposals of their own on how to overcome what were seen as the limitations of the options and solutions proposed.

3.1.4. Inception Impact Assessment

In July 2016, an Inception Impact Assessment (European Commission - Inception Impact Assessment TPD, 2016) was published as a first step in the impact assessment process of policy options for establishing and operating an EU Tracking and Tracing System.

According to the analysis, there are key decision points that must be addressed in the process of selecting the best possible solution for the implementation of Articles 15 and 16 of the TPD. A summary of the policy options is presented below.

Tracking and tracing	Security

[4] Philip Morris, BAT, JTI, and Imperial

				features
Who?	Where?	How?	When?	How?
(A) Governance model	**(B) Data storage location**	**(C) Allowed data carriers**	**(D) Allowed delays in reporting events**	**(S) Method of adding a security feature**
(A1) Industry operated solution	**(B1)** Centralised data storage	**(C1)** System with a single data carrier	**(D1)** Real-time (or limited delay) reports	**(S1)** Affixing
(A2) Third party operated solution	**(B2)** Decentralised data storage	**(C2)** System with a limited variety of data carriers	**(D2)** Once daily reports	**(S2)** Printing or integrating through a different method
(A3) Mixed solution (industry and third party)	-	**(C3)** Free system allowing any existing data carrier	**(D3)** Once weekly reports	**(S3)** Mixed solution

Table 5: Policy options, as per the Inception Impact Assessment

According to the Inception Impact Assessment, the blocks of options A, B, C, D, and S are largely independent of each other, and any combination of them should be possible. Thus, the optimal solution may combine elements from several options of the Feasibility Study in order to ensure compliance with all TPD requirements.

3.1.5. Public Consultation

The main aim of the Public Consultation (European Commission - Public consultation TPD, 2016) was to seek input from the general public and interested parties on the various policy options presented in the Inception Impact Assessment for implementing an EU Tracking and Tracing System and security features.

The Public Consultation was made available online from 29 July to 4 November 2016 and the targeted groups were the general public/consumers of tobacco products; retailers of finished tobacco products; manufacturers of finished tobacco products; wholesalers and distributors of finished tobacco products; providers of solutions for operating traceability, security feature, or data storage systems; and governmental and non-governmental organisations active in the area of tobacco control or the fight against illicit trade. In total, 351 respondents submitted replies to the survey via the European Commission website.

The Public Consultation aimed to:

- Gain insight into which policy options would be most capable of fulfilling TPD requirements whilst imposing the least amount of burden on the stakeholders concerned;
- Gain realistic estimations of the financial impact that the envisaged policy options would have on stakeholders;
- Gain insight into the impact of the envisaged policy options on SMEs;
- Seek the feedback of consumers regarding any aspects of particular relevance for them.

3.2. Implementation Study

3.2.1. Objectives

The Implementation Study for EU Tobacco Traceability (hereafter 'Implementation Study') will assist the European Commission in preparing the Implementing and Delegated Acts aiming to:

- Develop and implement an EU Tracking and Tracing System of tobacco products at unit packet level in line with Article 15 of the TPD, and as requested by the TPD;
- Develop and implement a system that ensures that all unit packets of tobacco products that are placed on the EU market carry a tamper-proof security feature composed of visible and invisible elements, in line with Article 16 of the TPD, and as requested by the TPD.

3.2.2. Scope

To achieve the proposed goals, the Implementation Study is divided into four work packages. Work Package 1 focused on completing the technical knowledge base acquired in the Feasibility Study. Work Package 2 is about the high level design of the optimal system. Work Package 3 focuses on all the technical requirements for the implementation of the Tracking and Tracing System and security features, as per Articles 15 and 16 of the TPD. Work Package 4 consists of the preparation of the final report.

The figure below presents the different tasks of the work packages.

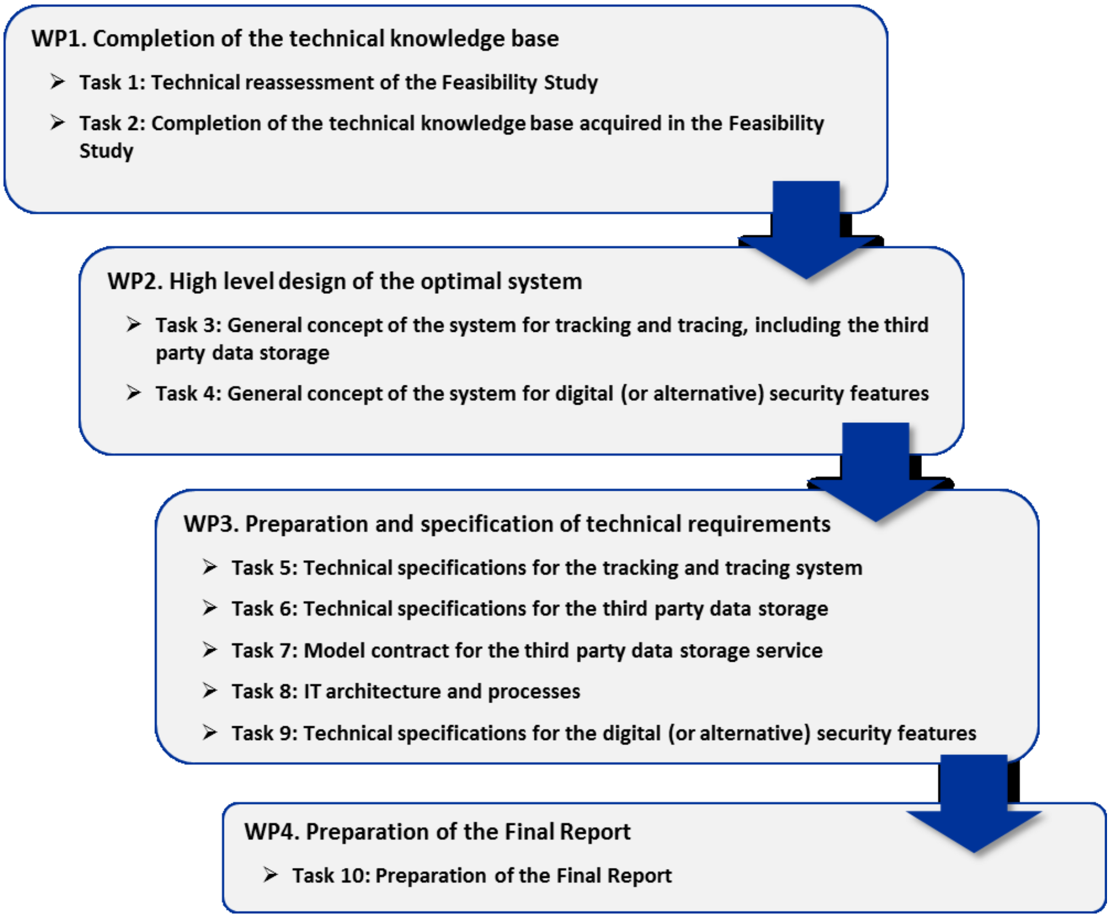


Figure 8: General overview of the Implementation Study Work Packages

3.2.3. Work Package 1

Work Package 1 aimed at completing the technical knowledge base, and setting the baseline for the high level design of the Tracking and Tracing System.

3.2.3.1. Methodology

The methodology of this work package consisted of the analysis of the Targeted Stakeholder Consultation, the Inception Impact Assessment, and the Feasibility Study, in order to identify the most relevant information and produce an interim report containing a complete technical knowledge base. This set the baseline for the cost-benefit analysis and the high level design of the Tracking and Tracing System.

3.2.3.2. Outcome of Work Package 1

Interim Report I was the outcome of Work Package 1. The first part of this report focused on the technical reassessment of the Feasibility Study, where the options proposed for the Tracking and Tracing System and for security features were critically analysed.

Regarding the Tracking and Tracing System, and despite having stated that the benefits outweigh the costs in all options proposed, the Feasibility Study did not choose a preferred option amongst those proposed. This led to the selection of a different range of options than the ones analysed in the Inception Impact Assessment.

Regarding the security features, a great deal of research was conducted in the Feasibility Study, which contains (generically) all of the options for security features currently available on the market. However, this analysis was not transposed into the options proposed at the end of the Feasibility Study, which were all based on affixed paper stamps.

Given the constraints on both the Tracking and Tracing System options and the security features, several limitations were identified in the cost-benefit analysis. A further review of the cost-benefit analysis was carried out in Work Package 2.

A major recommendation for the high level design of the Tracking and Tracing System is the consideration of policy options, as elaborated in the Inception Impact Assessment. The intention of the Inception Impact Assessment is to conduct a new analysis, which considers the trade-offs that each option presents (e.g. "concerning (B) data storage model, a decentralised data storage may be easier to implement and maintain, but with a centralised data storage it may be easier to treat information and generate reports").

The second part of Interim Report I focused on the completion of the technical knowledge base acquired in the Feasibility Study. The research conducted focused on the Tracking and Tracing System and on data storage, since the security features were already largely, if not completely, covered in the Feasibility Study.

Concerning the Tracking and Tracing System, the technical knowledge base includes an initial estimation of sizing of the data carrier according to the information required by the TPD. From this sizing estimation, the data carrier standards that can encode the data elements of the unique identifier required by the TPD can be inferred. The report also provides an overview of current industry trends, such as the use of blockchains as a storage alternative and the mapping of sector-specific Electronic Product Code Information Services (EPCIS) messages that are exchanged through the Representational State Transfer (REST) architectural style.

Regarding data storage, the technical knowledge was complemented with improvements on the sizing estimation of the data storage, the inclusion of the possibility of having computing resources close to the traceability data (in the "Bid process considerations" section), and the inclusion of requirements related to the communications network performance (in the "General requirements for software/ hardware/ hosting services" section).

3.2.4. Work Package 2

The Work Package 2 focused on the high level design of the optimal system.

3.2.4.1. Methodology

In order to assess the alternatives of the different policy options, a three-level approach was defined for their scoring (policy options alternatives, selection criteria, and evaluation criteria). This is illustrated in Figure 9.

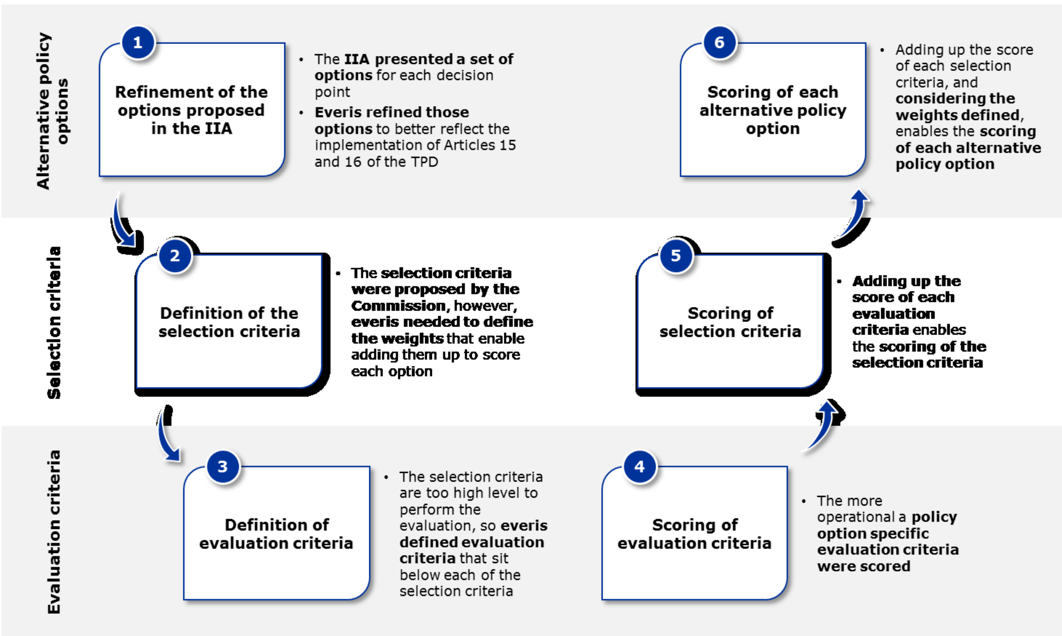


Figure 9: High level view of the approach followed

The methodology first focused on the refinement of the policy options proposed in the Inception Impact Assessment. As a result, the range of alternatives was extended for two policy options, namely '(B) Data storage model', and '(C) Allowed data carriers', as shown in the table below:

Tracking and Tracing System	Security features

Who?	Where?	How?	When?	How?
(A) Governance model	**(B) Data storage model**	**(C) Allowed data carriers**	**(D) Allowed delays in reporting events**	**(S) Method of adding a security feature**
(A1) Industry operated solution	**(B1)** Centralised model	**(C1)** System with a single data carrier for all identification levels	**(D1)** Near real-time reports	**(S1)** Affixing
(A2) Third party operated solution	**(B2)** Decentralised model per manufacturer/ importer	**(C2)** System with a single data carrier per identification level and optional data carriers for aggregation packaging levels	**(D2)** One-day delay reports	**(S2)** Printing or integrating through a different method
(A3) Mixed solution (industry and third party)	**(B3)** Decentralised model per Member State	**(C3)** System with a limited variety of data carriers for all identification levels	**(D3)** One-week delay reports	**(S3)** Mixed solution
-	**(B4)** Combined model: centralised for surveillance and decentralised for recording per manufacturer/ importer	**(C4)** System with limited variety of data carriers for all identification levels and optional data carriers for aggregation packaging levels	-	-
-	-	**(C5)** Free system allowing any existing approved data carrier	-	-

Table 6: Refined policy options, based on the Inception Impact Assessment

The next step was to define the selection criteria of the policy options to be evaluated on the basis of the tender specifications. These were split in two groups: primary requirements and secondary requirements. The first group of requirements concerned the full compliance of the alternative with Articles 15 and 16 of the TPD and Article 8 of the FCTC protocol. The second group of requirements were the selection criteria regarding the technical feasibility, interoperability, ease of operation, system integrity, system security, potential of reducing illicit trade, burden for economic operator, and burden for public authorities.

These selection criteria enabled a standard comparison and, ultimately, identification of the optimal solution. The selection criteria were given different weights and then added up, resulting in a final score for each option.

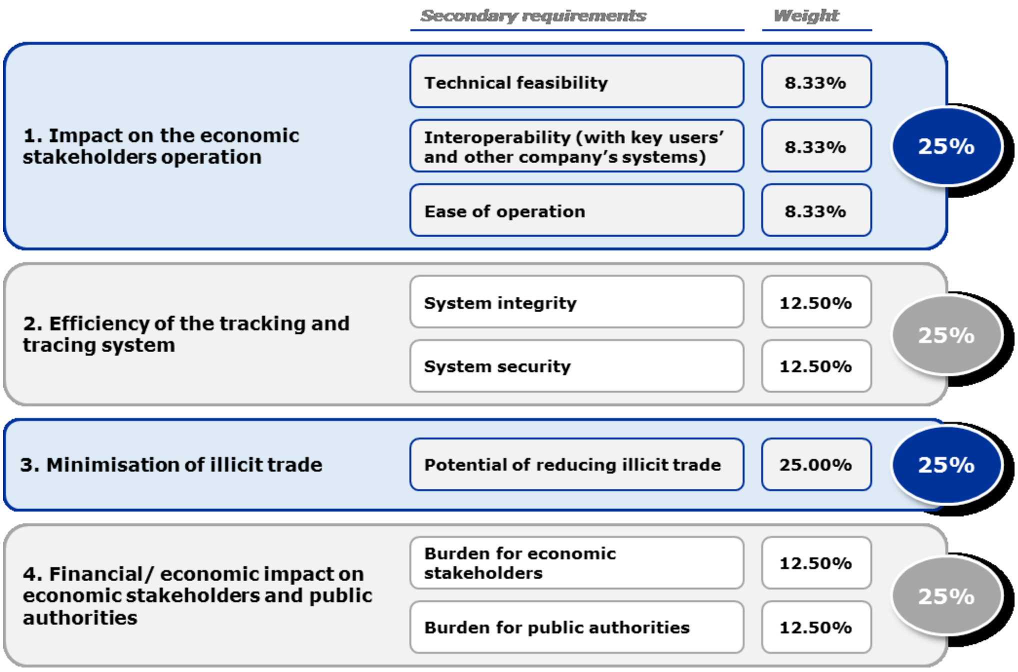


Figure 10: Weighting of the secondary requirements

The final score of each policy option was obtained by multiplying the score of each selection criteria by its respective weight. To increase and ensure the adequate level of precision of each policy option, a set of evaluation criteria was defined specifically for each option.

The scoring of the evaluation criteria was the basis of the whole scoring process. For the purpose of this evaluation, an eight-piece scoring model was defined.

In the specific case of the primary (mandatory) requirements, the only applicable scoring options were 0 and 100%, meaning that the option either complies with the mandatory requirement or does not, and is thereby cast out of the evaluation. For the secondary (optimisation) requirements, each option is rated 0 – 12.5 – 25 – 37.5 – 50 – 62.5 – 75 – 87.5 - 100.

The scoring of each option in the evaluation criteria defined is accompanied by a detailed justification, which describes how each option ranks in comparison to the others.

After scoring each option in the evaluation criteria, the process of scoring the selection criteria was simply to add their specific evaluation criteria, weighted homogeneously. With the results of this process, it was possible to see which option ranked better in each selection criterion.

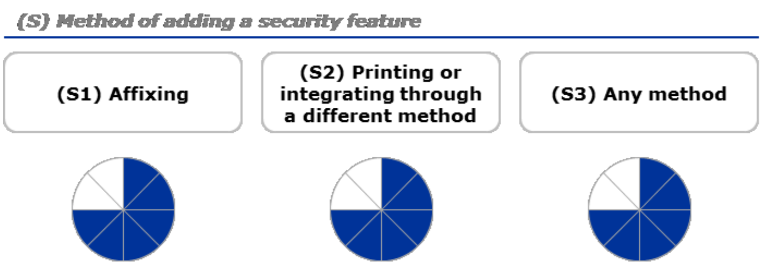


Figure 11: Scoring of a selection criterion (illustrative)

Finally, after combining the scoring of the selection criteria with the defined weights, a total score was given for each policy option. With this result, the option that best fits the requirements defined by the European Commission for each decision point was identified.

The total score of each option was also represented as a radar chart[5], which enables the positioning of the options against each other and the assessment of strengths and weaknesses.

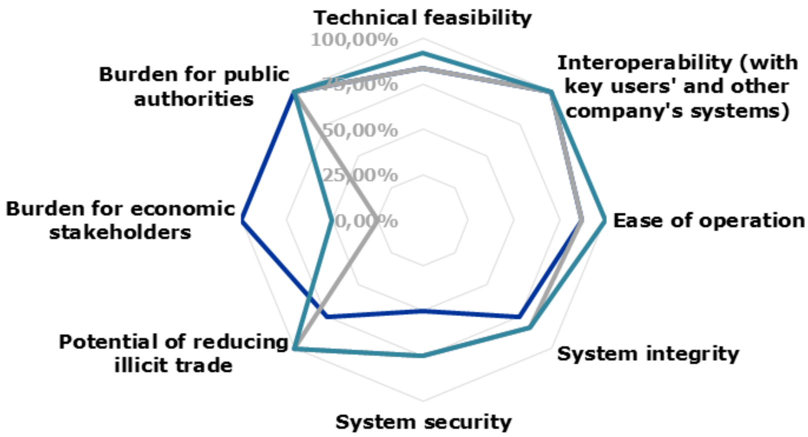


Figure 12: Radar chart for the final score of the policy options (illustrative)

3.2.4.2. Outcome of Work Package 2

The activities of Work Package 2 were distributed in three parts:

1. Definition and characterisation of all policy options under evaluation for the Tracking and Tracing System and for the security features applied to unit packets of tobacco products. These options are based on propositions from the Inception Impact Assessment, and were refined with our expertise and the knowledge gathered during the implementation of Work Package 1. The objective of this first part was to ensure a clear understanding of all options considered, in order to provide a basis for evaluation.
2. Detail the assessment of the evaluation criteria for the five decision points, to allow ranking of the different options in each decision point and proposing the optimal high level design of the Tracking and Tracing System. The policy options were evaluated against a set of selection criteria predefined by the European Commission and distributed in two groups:

[5] The radar charts only contain the eight secondary requirements, because no weighting was defined for the two primary requirements – these function as a Boolean variable, without an optimisation objective.

- Primary requirements: Options that do not fulfil these requirements were discarded from the final selection even if they score higher than the other options for the secondary requirements:
  - Full compliance with Articles 15 and 16 of the TPD and Article 8 of the FCTC Protocol;
- Secondary requirements: The objective was to select the option that fulfils the selection criteria in the most optimal way, taking into consideration:
  - Technical feasibility;
  - Interoperability (with key users' and other companies' systems);
  - Ease of operation;
  - System integrity;
  - System security;
  - Potential of reducing illicit trade;
  - Burden for economic stakeholders;
  - Burden for public authorities.

3. Description of several key elements of the future Tracking and Tracing System, including the cost-benefit analysis, business process diagram, system architecture, sequence diagrams, and data flow diagram.

The results of the assessment of the policy options led to the high level optimal system presented in the table below, which demonstrates that a feasible solution fulfilling the TPD and FCTC Protocol requirements exists within the boundaries set by the Inception Impact Assessment.

Tracking and tracing				Security features
Who?	**Where?**	**How?**	**When?**	**How?**
(A) Governance model	**(B) Data storage model**	**(C) Allowed data carriers**	**(D) Allowed delays in reporting events**	**(S) Method of adding a security feature**
(A1) Industry operated solution	(B1) Centralised model	**(C1)** System with a single data carrier for all identification levels	**(D1) Near real-time reports**	**(S1)** Affixing
(A2) Third party operated solution	**(B2)** Decentralised model per manufacturer/ importer	(C2) System with a single data carrier per identification level and optional data carriers for aggregation packaging levels	**(D2)** One day delay reports	**(S2)** Printing or integrating through a different method
(A3) Mixed solution (industry and third party)	**(B3)** Decentralised model per Member State	**(C3)** System with a limited variety of data carriers for all identification levels	**(D3)** One-week delay reports	**(S3) Mixed solution**
-	**(B4) Combined model: centralised for surveillance and decentralised for recording per manufacturer/ importer**	**(C4) System with limited variety of data carriers for all identification levels and optional data carriers for aggregation packaging levels**	-	-
-	-	**(C5)** Free system allowing any existing approved data carrier	-	-

Table 7: Optimal system based on the policy options

3.2.5. Work Package 3

Work Package 3 represented the preparation and specification of technical requirements.

3.2.5.1. Methodology

In order to provide a comprehensive and detailed description of the different topics addressed in this work package, the following methodologies and standards have been applied:

Topic	Methodology/standard
Project Charter	PM^2 Methodology – Project Charter template
Business Case	PM^2 Methodology – Business Case template
Business Process Diagrams	Business Process Model and Notation (BPMN) version 2.0 standard (OGG - BPMN 2.0, 2011)
System Users	RACI (Responsible, Accountable, Consulted, and Informed) matrix model
Use Case	RUP@EC – Use Case specification artefact
System Architecture	RUP@EC – Architecture artefact

Sequence Diagrams	UML standard sequence diagram notation ISO/IEC 19505-1:2012 (ISO/IEC 19505-1:2012 UML, 2014)
Data Flow Diagrams	DeMarco & Yourdon data flow diagrams methodology (Yourdon & DeMarco, 2017)
Requirements Specification	RUP@EC – System-wide requirements specification artefact
Contingency Plans	NIST - Contingency Planning Guide for Federal Information Systems (Swanson, Marianne; Bowen, Pauline; Phillips, Amy Wohl; Gallup, Dean; Lynes, David, 2010)
Control Mechanisms	Failure mode and effects analysis (FMEA) (SAE J-1739 - FMEA Standard, 2009)
Security Policy	ISO/IEC 27000 family of standards
Data Dictionary	Tobacco products data dictionary to submit information of tobacco products as required by the TPD

Table 8: Methodologies applied to elaborate the contents of the Implementation Study

3.2.5.2. Outcome of Work Package 3

The activities on Work Package 3 were distributed into five parts:

- Technical specifications for the Tracking and Tracing System
- Technical specifications for the third party data storage
- Model contract for the third party data storage service
- IT architecture and processes
- Technical specifications for the digital (or alternative) security features

3.2.6. Work Package 4

Work Package 4 corresponded to the preparation of this final report.

3.2.6.1. Methodology

The methodology consisted of the analysis, compilation and refinement of the outcome of the previous three work packages, in order to identify and extract the most relevant information of each report, and finally to produce this final report containing the conclusion of the overall study.

3.2.6.2. Outcome of Work Package 4

It includes the main analyses and conclusions obtained in the previous three Work Packages, being structured into three main sections:

- General concept of the system
- Technical specifications of the Tracking and Tracing System
- Technical specifications of the security features

4. General concept of the System

This chapter on the general concept of the System is divided into different sections that aim to provide an outlook of the proposed Tracking and Tracing System. The sections are as follows:

- Project charter: The project charter includes fundamental information used to establish the basis of the future Tracking and Tracing System, such as its legal basis, success criteria, scope, assumptions, constraints, and a roadmap.
- High level solution design: The high level solution design presents a summary of the definition and characterisation of all policy options under evaluation, and selects the best options in each decision point based on the evaluation criteria.
- Cost-benefit analysis: The cost-benefit analysis gives a summary of an extensive analysis that was done in Interim Report II, which describes the benefits associated with the effective implementation of the proposed measures, together with the costs of the new Tracking and Tracing System in the entire tobacco supply chain.

Additionally, Chapter 1 of Annex II "*General elements of the Tracking and Tracing System*" includes five sub-sections providing the detailed definition of the needed elements for the correct functioning and definition of the system. It includes: process map, registration processes, business process diagrams, system users, use cases, control mechanisms, contingency plans, and system security plan.

4.1. Project Charter

The Project Charter provides a high level view of the more detailed system requirements. The following sections ('Solution description' and 'Governance and stakeholders') are intended to capture the "essence" of the envisaged system in the form of high level requirements and constraints, thereby providing an overview of the final configuration of the system.

The Project Charter will serve as a key decision element in the project approval process, which communicates the general framework ("why and what") for the Tracking and Tracing System, and will be a gauge against which all future decisions can be validated.

4.1.1. Solution description

The solution description section aims to highlight the legal basis, benefits, costs/effort and funding source, success criteria, scope, assumptions, constraints, and roadmap of the future Tracking and Tracing System.

4.1.1.1. Legal basis

This initiative implements Articles 15 and 16 of the TPD. The power to adopt implementing and delegated acts is conferred to the European Commission by Article

15(11), 15(12) and 16(2) of the TPD. An additional check was already carried out in the impact assessment of the TPD and compliance with the principle has been confirmed by the Court of Justice of the EU.[6]

Therefore, in the absence of the adoption of these acts, the Commission would not meet its obligations under the above-mentioned provisions.

In addition, the European Union, which is a Party of both the FCTC and the FCTC Protocol, has committed to establishing a Tracking and Tracing System for tobacco products.[7]

4.1.1.2. Benefits, cost, effort and funding source

The content of this section is transferred to the sub-section *"4.3 Cost-benefit analysis"*, which presents a broader and more detailed explanation of the benefits and cost associated with the implementation of the Tracking and Tracing System.

4.1.1.3. Success criteria

The project must meet the following milestones to be successful:

1. A Tracking and Tracing System for cigarettes and RYO tobacco, which meets the requirements of Article 15 of the TPD, must be implemented **before 20 May 2019.**
2. Security features for cigarettes and RYO tobacco, which meet the requirements of Article 16 of the TPD, must be implemented **before 20 May 2019.**
3. A Tracking and Tracing System for tobacco products other than cigarettes and RYO tobacco, which meets the requirements of Article 15 of the TPD, must be implemented **before 20 May 2024.**
4. Security features for tobacco products other than cigarettes and RYO tobacco, which meet the requirements of Article 16 of the TPD, must be implemented **before 20 May 2024**.

4.1.1.4. Scope

The scope of the project is to implement an effective system for tracking and tracing tobacco products and for security features, as envisaged in Articles 15 and 16 of the TPD.

The scope includes tobacco products that are manufactured inside of the European Union as well as tobacco products that are manufactured outside of the European Union but are destined for or placed on the EU market. The obligations laid down in this system apply to all economic operators involved in the trade of tobacco products, from the manufacturer to the last economic operator before the first retail outlet.

---

[6] Judgment of 4 May 2016, *Philip Morris Brands and others* (C-547/14) ECLI:EU:C:2016:325.
[7] Article 8(2) Protocol.

The tobacco products manufactured outside of the European Union that are not destined for or placed on the EU market are excluded from the scope of the project. All economic operators before the manufacturers (tobacco growers, transporters of tobacco plants, etc.) and the retailers (at the point of sale) are excluded from the scope of the project.

Tobacco products produced in the European Union but intended to be exported to non-EU countries do not require a security feature in the terms of Article 16 of the TPD.

4.1.1.5. Assumptions

The main assumption is that all the legislative work will be finalised by the end of December 2017, so that the technical roll-out can effectively begin in the beginning of 2018. The legislative work comprises two Implementing Acts and one Delegated Act.

Additionally, it is assumed that all economic operators affected by the TPD will adapt their capabilities to be able to meet the requested measures, not only for the solutions needed for the correct marking of unit packets with the unique identifier, but also the implementation of the anti-tampering solutions to verify the non-manipulation of the system and the adaptation of their internal information systems to achieve the required level of information exchange. The distribution chain operators will also need to adapt their operations to meet the demands of the Tracking and Tracing System.

4.1.1.6. Constraints

The main constraint highlighted by the different stakeholders consulted is the ambitious and demanding schedule set by the TPD, which requires the Tracking and Tracing System to be implemented by May 2019 for cigarettes and RYO tobacco and by May 2024 for other tobacco products.

Some stakeholders have questioned this ambitious timeline in regard to the development of the technical roll-out.

The different nature of the processes involved in the manufacturing of tobacco products creates the need to develop solutions for all type of stakeholders. Manufacturers of cigarettes must be differentiated from manufacturers of other tobacco products, taking into account the production speed and the automation of the processes for each of them.

There are also constraints for importers, who have to communicate to their suppliers regarding the need to implement the solutions to mark all unit packets of tobacco products, or mark them by themselves, following the consequent process of aggregation.

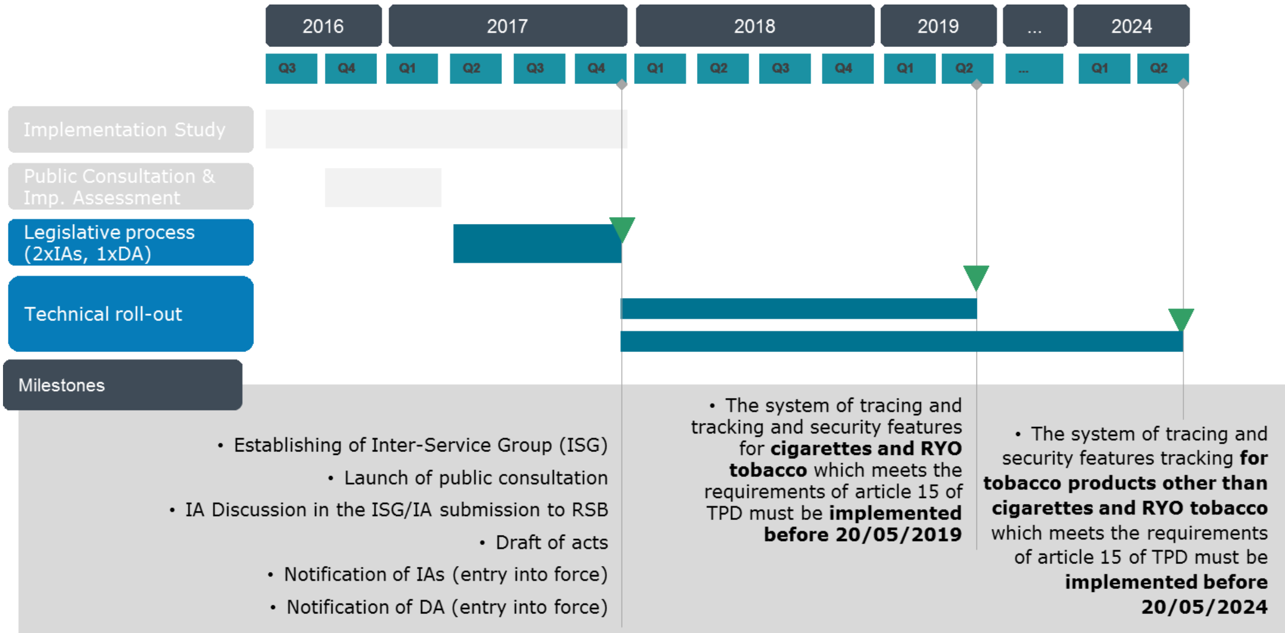
4.1.1.7. Roadmap

With the objective of defining the Implementing and Delegated Acts, the following must be achieved:

- Develop and implement an EU Tracking and Tracing System for tobacco products at unit packet level, in line with Article 15 of the TPD, and as requested by the TPD;
- Develop and implement a system that ensures that all unit packets of tobacco products, which are placed on the EU market, carry a tamper-proof security

feature composed of visible and invisible elements, in line with Article 16 of the TPD, and as requested by the TPD.

The roadmap highlighting the main milestones to be achieved is presented below:



4.1.2. Governance and stakeholders

The Tracking and Tracing System for tobacco products at EU level is a complex ecosystem, with multiple stakeholders involved and a high volume of products commercialised, and is very demanding from a technical perspective. Furthermore, the illicit trade of tobacco products is a strong and continuous threat, with criminal techniques that constantly evolve in order to overcome the system aiming to reduce such trade.

For all these reasons, it is advised to establish a strong governance that can oversee the System in the short, medium and long term; and also to ensure the constant evolution of the System to guarantee its effectiveness in fighting illicit trade. This governance must be achieved by clearly allocating the responsibilities of the management and implementation of the System to the different actors.

4.1.2.1. Allocation of responsibilities on the management and implementation of the System

A clear allocation of the responsibilities for the implementation and management of the System to the different actors, aligned to the spirit of the TPD, will be necessary.

The allocation should be as follows:

	Selected / proposed by	Approved by	Contractual relation
ID Issuer(s)	It is advised that the selection of the ID Issuer is done by the competent authorities of each of the 28 EU Member States, ensuring that this critical process – the generation of the serial numbers – is always under control of the competent authorities. Each Member State shall select an ID Issuer, or some of them could create clusters to jointly contract an ID Issuer, for the sake of efficiency and economies of scale. This may result in the selection of up to 28 ID Issuers.	Competent authorities of the Member States	Between the industry and the ID Issuer(s), based on flat fees per serial numbers generated, with no access or registration costs.
Primary Data Storage	Manufacturers and importers shall propose the providers of the Primary Data Storage.	As required by art. 15.8 of the TPD, the European Commission must approve the suitability, independence and technical capabilities, as well as the contract, of the third party providing the Primary Data Storage.	Contract between the manufacturers / importers and the providers of Primary Data Storage.
Surveillance Data Storage	Providers of Primary Data Storage.	As required by art. 15.8 of the TPD, the European Commission must approve the suitability, independence and technical capabilities, as well as the contract, of the third party providing the Primary Data Storage.	Contracted jointly by the primary data storages providers, with the costs of the Surveillance Data Storage charged to the manufacturers and importers.
External Auditors	As required by art. 15.8 of the TPD, the activities of the provider(s) of the data storages shall be monitored by an external auditor, who is proposed and paid by the tobacco manufacturers (and importers).	As required by art. 15.8 of the TPD, the European Commission must approve the external auditors proposed by the industry.	Contract between the manufacturers and importers and the external auditors.

	Selected / proposed by	Approved by	Contractual relation
Anti-tampering devices (on verification phase)	As further developed in Chapter 5, an external third party should be in charge of installing and operating the anti-tampering solution (in verification phase) at the manufacturing sites. The manufacturers and importers shall be allowed to select the external third party provider of anti-tampering solutions from a list of pre-approved solution providers by the competent authorities of each Member State.	The competent authorities of each Member State shall pre-approve and validate a list of external third party providers of anti-tampering solutions, based on their independence and technical capabilities.	Contract between the manufacturers and importers and the external third party providers of anti-tampering solutions.
Security Features	The competent authorities of the Member States shall be responsible for the selection and approval of the security features to be applied on the tobacco products. The security features must be, irremovable, printed or affixed, indelible and not hidden or interrupted and composed of visible and invisible elements, as requested by art. 16.1 of the TPD. The European Commission shall define in its Implementing Acts the technical standards for the security features and the rotation rules, as requested by art. 162 of the TPD.		Contracted by the competent authorities of the Member States, through the entities/agencies with competences on security features.

4.1.2.2. Stakeholders

The *general public*, together with the public authorities, is the group most affected by the issues at stake. In the absence of effective tracking and tracing and security features, tobacco products not compliant with the TPD and other EU and national legislative provisions would be available to the general public in considerable quantities.

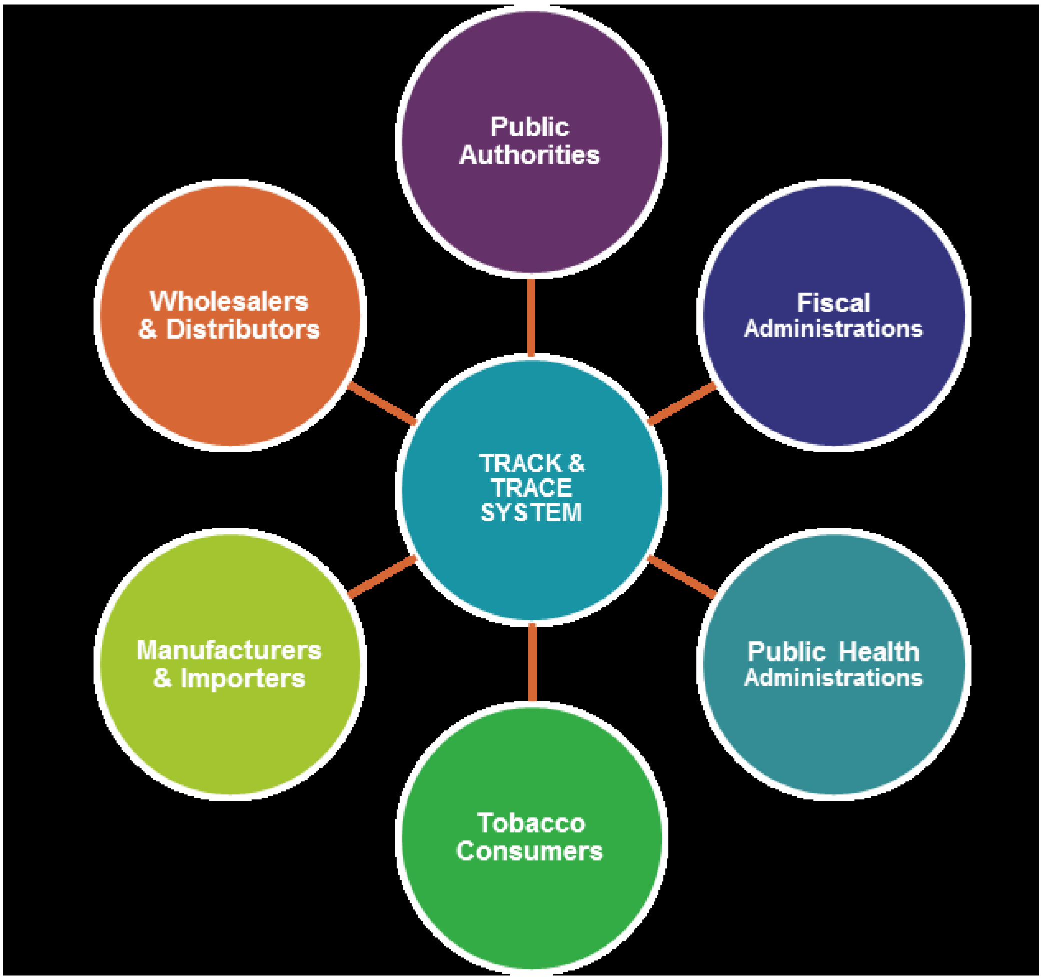
Governments and society are also affected by the issues at stake, in terms of health protection and the costs associated with treating smoking related diseases, as well as loss of budgetary revenues resulting from unpaid taxes on these illicit tobacco products.

Manufacturers and importers, as well as economic operators involved in the supply chain of tobacco products are affected by the lack of a Tracking and Tracing System. Indeed, the fact that illicit products are available to consumers reduces the quantity of legal products sold, resulting in economic losses for manufacturers and importers. Reducing the illicit supply is expected to direct a part of the demand towards the legal supply chain.

The key actors of the tobacco supply chain are:

- *Manufacturers*: any natural or legal person that acquires raw materials and processes them in order to produce a tobacco product, which is then sold to wholesalers and retailers (and importers in the case of manufacturers outside the EU);
- *Importers:* owner of, or a person having the right of disposal over, tobacco products that have been brought into the territory of the EU;

- *Wholesalers/distributors:* any natural or legal person that acquires tobacco products from manufacturers or importers and either sells them to a distributor or to an agent / another wholesaler.



4.2. High level solution design

This section presents the high level design of the Tracking and Tracing System as the combination of the selected policy options presented in Interim Report II. The policy options were mainly drawn from the results of the Inception Impact Assessment and from everis expertise and specific knowledge acquired during Work Packages 1 and 2, which further refined the options. Chapter 1 of Annex I*: "Technical evaluation of policy options"* extensively defines and analyses each policy option, selecting the most adequate alternatives, which are introduced in the table below.

Tracking and tracing				**Security features**
Who?	**Where?**	**How?**	**When?**	**How?**
(A) **Governance model**	**(B)** **Data storage model**	**(C)** **Allowed data carriers**	**(D)** **Allowed delays in reporting events**	**(S)** **Method of adding a security feature**
(A3) Mixed solution (industry and third party)	**(B4)** Combined model: centralised for surveillance and	**(C4)** System with limited variety of data carriers for all	**(D1)** Near real-time reports	**(S3)** Mixed solution

	decentralised for recording per manufacturer/ importer	identification levels and optional data carriers for aggregation packaging levels		

Table 9: Selected policy options based on the Inception Impact Assessment

4.2.1. Governance model: Mixed solution

In this option, the different processes and tasks for the operation of the Tracking and Tracing System are split between by the industry and independent third parties, resulting in a mixed solution. This alternative allows full control of the System (as required by the FCTC Protocol) with minimum disruptions to the production process.

The allocation of tasks must ensure that the control of the system by the competent authorities is maintained at all times, splitting responsibilities per function:

- Generation of unique identifier: the codes for the unique identifiers of tobacco products are generated by an independent third party (under the control and supervision of the competent authorities) or by the competent authorities themselves.
- Printing or affixing data carriers: the industry performs the activities of printing or affixing the codes.
- Scanning or verifying data carriers:
    - Manufacturers and importers: the industry may perform the technical task of scanning/verification of the codes, but a third party may be asked to install anti-tampering devices in order to provide the competent authorities with full control of the system.
    - Distributors: The industry may perform the scanning/verification of the codes, without installing additional anti-tampering devices.

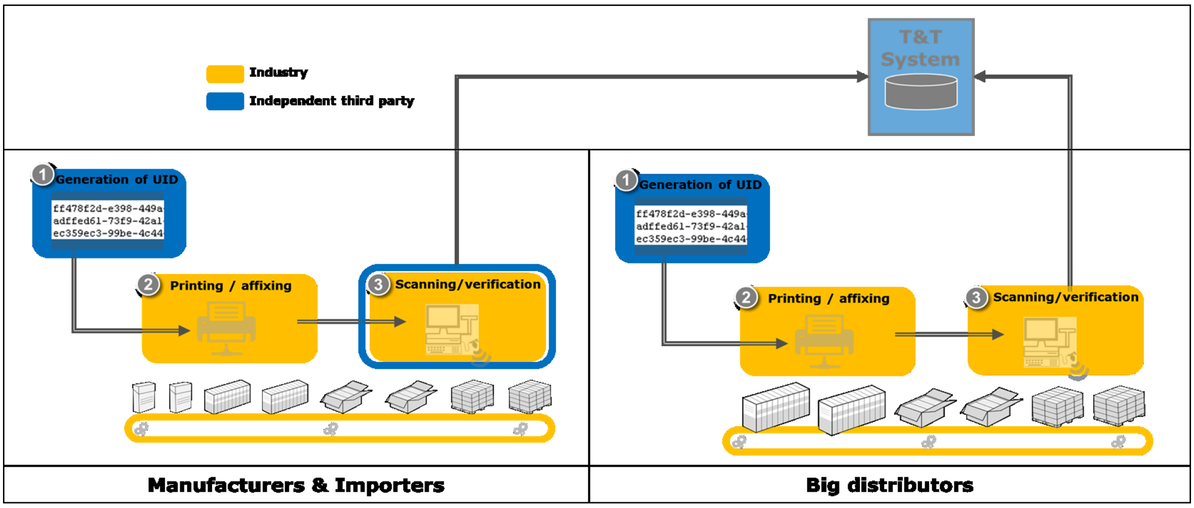


Figure 13: Proposition of optimal allocation of the areas of responsibilities and functions

4.2.2. Data storage models: Combined model – centralised for surveillance and decentralised for recording (per manufacturer/ importer)

This model comprises an independent central surveillance solution at EU level and a group of independent data storage solutions per manufacturer/importer, integrating benefits from the centralised (i.e. efficient access to the comprehensive logical view of data) and decentralised (i.e. efficient data processing and writing) models.

Hence, the aim of this model is to decouple read accesses from write accesses, splitting such responsibilities between the following solutions:

- The data storage solutions: They behave as intermediate layers focused on data recording, processing and storing. Each data storage solution processes data exclusively related to a specific manufacturer or importer, and is later synchronised with the central surveillance solution.
- The independent central surveillance solution: It offers a comprehensive logical view of all relevant data based on a local data storage solution with data that has been synchronised previously from the distributed data storage solutions.

The logical components of this model are depicted below:

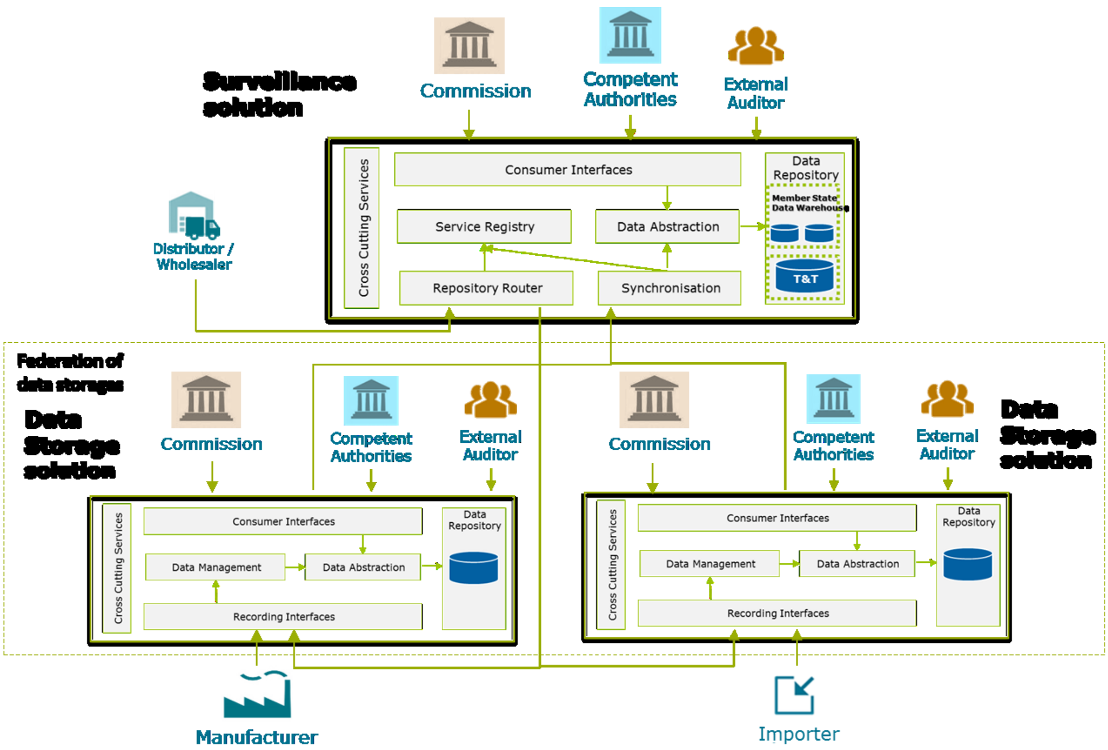


Figure 14: Combined model: centralised for surveillance and decentralised for recording

4.2.3. Allowed data carriers: System with limited variety of data carriers per identification level and optional data carriers for aggregation packaging levels

This option enables the economic operators to choose between an authorised variety of data carriers for the unit packet and all aggregation packaging levels, where the data carriers for each identification level may differ. The proposed data carriers will not affect the integrity of other data carriers currently placed in the unit packets.

Additionally, in order to facilitate scanning activities along the distribution chain operators, it is optional to add approved data carriers for the aggregation packaging levels. The following image depicts the system with a limited variety of data carriers for the different identification levels (unit packet, carton, master case and pallet).

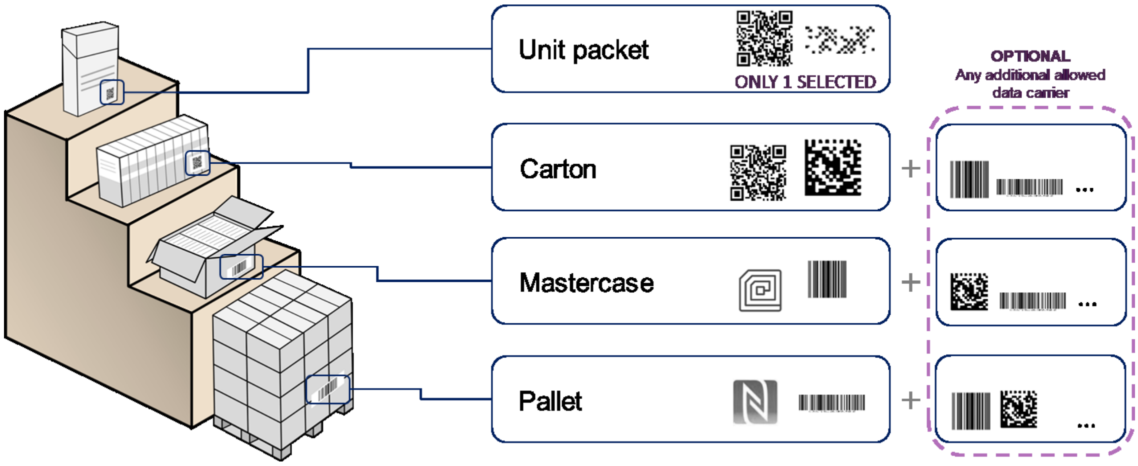


Figure 15. Description of the system with limited variety of data carriers per identification level and optional data carriers for aggregation packaging levels

4.2.4. Allowed delays in reporting events: Near real-time reports

In this option, the economic operator must commit to reporting event messages on a near real-time basis (assuming 60 minutes as maximum delay), meaning that low latency should exist between the event occurrence and the transmission to the data storage solution.

Near real-time data reporting delay has the following implications:

- A low-latency business enterprise. The economic operator production line and data transmit channels must be able to access, propagate and process the data in low latency. That means that any approval or confirmation of the event is done through management software (such as an ERP), and the event reporting must be concluded within this allowed delay.
- A continual input and output of data being processed in a short period of time (near real-time).
- A highly fault-tolerant reporting system on the economic operators' side, with the ability to recover from data report process failure, in order to keep the same level of performance and deal with any unforeseen problems, such as connection downtimes.
- A small amount of data sent several times, thereby reducing the volume of data to be sent per transmission, which means an even and nearly balanced volume of data transmission during a given timeframe.
- The possibility for law enforcement to proactively analyse and react upon a potentially suspicious event reported.

4.2.5. Method of adding a security feature: Mixed solution

The mixed solution enables the use of at least one printed or affixed security feature. This solution will minimise the implementation impact, while complying with all requirements of Article 16(1) of the TPD. Furthermore, in order to comply with Article 16(2) of the TPD regarding the rotation of security features, affixing is to be understood in the broader meaning of "attaching in any way" rather than a more restrictive meaning such as "labelling" or "sticking".

The choice of the method of application will depend mainly on the following drivers:

- The type of tobacco product and packaging: Printing or integrating security features through a different method is more suitable and more cost efficient for certain types of tobacco products or packaging. For other types of products or packaging, affixing the security features might be a better choice.
- Member States' preferences: This solution allows Member States to select the most suitable security features, taking into consideration the ones already available in their country and the associated processes.

4.3. Cost-benefit analysis

The cost-benefit analysis (European Commission - DG REGIO, 2014) is an analytical instrument for judging the economic and social advantages and disadvantages of an investment decision by assessing its costs and benefits and thus estimating the impact attributable to it.

This sub-section assesses the viability of the project implementation and analyses the benefit streams, the investment, and ongoing costs associated to the execution of the project.

Additionally, Chapter 2 of Annex I*: "Assessment for the calculation of the cost-benefit analysis"* includes a more detailed explanation of the calculations made for the development of this sub-section.

4.3.1. Benefit assessment

Illicit tobacco trade has been estimated to account for 11.26% (European Commission - TPD Inception Impact Assessment, 2016) of the total consumption of tobacco products. Implementing effective measures to control and fight against illicit trade will contribute to reducing the total consumption. The effect of this reduction is expected to be threefold (Reed, 2010):

- Some smokers will smoke less;
- Others will stop smoking altogether; and
- Smoking take-up will decline, increasing the number of non-smokers.

The benefits associated to the effective implementation of the proposed measures can be further classified by their nature: economic or social and environmental.

4.3.1.1. Economic benefits

The economic benefits are defined as the net income generated as the result of the implementation of the proposed measures. In this sense, the solution revenues and benefits are analysed using two main quantitative factors:

- Revenues from increase in legal sales
- Other economic benefits: reduction in costs associated to public health care and benefits derived from an increase in productivity.

Impact on illicit trade reduction

The estimation of the market size, both legal and illicit, is based on the TPD Inception Impact Assessment (European Commission - TPD Inception Impact Assessment, 2016). This report estimates the total consumption of manufactured cigarette in the 28 Member States to be 27.49 billion unit packets (assuming a unit packet contains an average of 20 cigarettes), while the illicit consumption is rated as 3.096 billion unit packets.

Consumption breakdown		
Legal Consumption ***(Millions of unit packets – Total EU28)***	**(A)**	**24,395.80**
Illicit Consumption ***(Millions of unit packets – Total EU28)***	**(B)**	**3,096.01**
Total Consumption ***(Millions of unit packets – Total EU28)***	**(C) = (A) + (B)**	**27,491.81**
% Illicit Consumption ***(% - Total EU28)***	**(D) = (B) / (C)**	**11.26%**
Source: (A): (European Commission - TPD Inception Impact Assessment, 2016) (B): (World Lung Foundation, 2015)		

Table 10: Consumption breakdown of tobacco products

The report further divides the illicit consumption into illicit whites, counterfeit, and other counterfeit and contraband (C&C), which was assumed to be 100% contraband for the purpose of the calculations.

Illicit Consumption		
Percentage of Illicit Whites ***(Average % for EU28)***	**(E)**	**34.63%**
Percentage of Counterfeit ***(Average % for EU28)***	**(F)**	**6.78%**
Percentage of Contraband ***(Average % for EU28)***	**(G)**	**58.59%**
Illicit Whites Consumption ***(Millions of unit packets – Total EU28)***	**(H) = (B) · (E)**	**1,025.33**
Counterfeit Consumption ***(Millions of unit packets – Total EU28)***	**(I) = (B) · (F)**	**248.62**
Contraband Consumption ***(Millions of unit packets – Total EU28)***	**(J) = (B) · (G)**	**1,822.06**
Source: (E), (F), (G): (Transcrime, Joint Research Centre on Transnational Crime, 2015)		

Table 11: Illicit consumption of tobacco products

The effective implementation of the proposed measures aims for a reduction in illicit trade to the order of 30% for contraband (European Commission - TPD Inception Impact Assessment, 2016), 10% for counterfeit, and 10% for illicit whites (European Commission - Feasibility Study, 2015), and this will serve as our baseline. Mapping the values presented for illicit trade with the baseline reduction, it is possible to quantify the total impact on the tobacco products market.

Estimated impact on illicit trade reduction I		
Reduction in consumption of Illicit Whites *(Millions of unit packets – Total EU28)*	(K) = (H) · 10%	102.53
Reduction in consumption of Counterfeit *(Millions of unit packets – Total EU28)*	(L) = (I) · 10%	24.86
Reduction in consumption of Contraband *(Millions of unit packets – Total EU28)*	(M) = (J) · 30%	546.62
Reduction in Illicit Consumption *(Millions of unit packets – Total EU28)*	(N) = (K) + (L) + (M)	674.01
Percentage of reduction in Illicit Trade *(%– Total EU28)*	(O) = (N) / (B)	21.77%
Percentage of reduction in Total Consumption *(%– Total EU28)*	(P) = (N) / (C)	2.45%

Table 12: Estimated impact on illicit trade reduction (I)

Assuming the baseline values, the solution can produce a reduction in illicit trade with a total impact on the tobacco products market of 674.01 million unit packs, representing a 2.45% reduction in total consumption.

This reduction in illicit trade results in one of two possible effects:

- An increase of sales in the legal market; and/or
- A portion of smokers that will reduce consumption, or even quit smoking.

In order to model the effects of the reduction in illicit trade, the concept of price elasticity is applied to the analysis. It represents the responsiveness of the quantity of tobacco products demanded, to a change in price. According to the value of -0.41, as the average price elasticity for the EU28, and given an increase of the price of 100% and the log-linear demand function, we can assume that:

- 75.15% of illicit tobacco would be replaced with legitimate tobacco products.
- 24.85% of illicit tobacco would not be replaced, because purchasers would either decide to reduce their consumption, or even quit smoking.

• Estimated impact on illicit trade reduction II		
GDP per capita in PPS	(Q)	100
Price elasticity	(R)	-0.41
Increase in the price of tobacco products	-	100%
Percentage of consumers that would now decide to reduce their consumption or even quit smoking *(Average % for EU28)*	(S) = function of (R)	24.85%

Percentage of consumers that would now purchase legitimate tobacco products ***(Average % for EU28)***	**(T) = 100% - (S)**	**75.15%**
Reduction in Total Consumption ***(Millions of unit packets – Total EU28)***	**(U) = (N) · (S)**	**164.05**
Increase in Legitimate Consumption ***(Millions of unit packets – Total EU28)***	**(V) = (N) · (T)**	**509.97**
Source: (Q): (Eurostat, 2016)		

Table 13: Estimated impact on illicit trade reduction (II)

Revenues from increase in legal sales

One of the expected revenues from the implementation of the solution is that the increase in legal tobacco sales will generate an increase in revenues (VAT, excise duty, EO's revenue).

Estimated impact on illicit trade reduction		
Price of a 20-cigarette pack of the most sold brand ***(Average price for EU28)***	**(W)**	**4.38 €**
Average VAT ***(Average % for EU28)***	**(X)**	**21.50%**
Excise duties as % of the price ***(Average % for EU28)***	**(Y)**	**57.68%**
EO's revenue as % of the price ***(Average % for EU28)***	**(Z) = 100% - (X) – (Y)**	**20.82%**
Impact on VAT ***(Millions of Euros – Total EU28)***	**(A') = (V) · (W) · (X)**	**528.84 M€**
Impact on excise duty ***(Millions of Euros – Total EU28)***	**(B') = (V) · (W) · (Y)**	**1,500.13 M€**
Impact on EO's revenue tax ***(Millions of Euros – Total EU28)***	**(C') = (V) · (W) · (Z)**	**525.47 M€**
Source: (W): (Transcrime, Joint Research Centre on Transnational Crime, 2015) (X): (European Comission - Taxation and Costumer Union, 2016) (Y): (European Commision - Excise duty tables, 2016)		

Table 14: Estimated impact on illicit trade reduction (III)

Combining the 509.97 million packs that would now be bought on the legal market, and taking into account the price of tobacco unit packets and the tax levels in each country, the implementation of the solution is expected to generate:

- 528.84 million euros as new tax revenues from VAT;
- 1.5 billion euros as new tax revenues from excise duties;
- 525.47 million euros as new revenues for the economic operators involved in the value chain of the tobacco products.

Other economic benefits

Additionally, the reduction of consumption generates different economic impacts on society. The main positive impact is the reduction in health care expenditure. Reduced tobacco consumption will also lead to lower health care costs and improved productivity due to fewer cases of absenteeism and premature retirement. These socio-economic benefits can be estimated with the following equations:

$$Decrease\ in\ healthcare\ expenditure\ (M€) = Coefficient_{Healthcare} \cdot \%Reduction\ tobacco\ consumption$$

$$Increased\ productivity\ (M€) = Coefficient_{Productivity} \cdot \%Reduction\ tobacco\ consumption$$

Estimated socio-economic benefits		
Healthcare expenditure coefficient	**(D')**	**25,300**
Increased productivity coefficient	**(E')**	**8,300**
Decrease in healthcare expenditure ***(Millions of Euros – Total EU28)***	**(F') = (D') · (S) · (P)**	**154.03 M€**
Increased productivity ***(Millions of Euros – Total EU28)***	**(G') = (E') · (S) · (P)**	**50.53 M€**
Source: (D') (E'): (European Commission - TPD Impact Assessment, 2012)		

Table 15: Estimated socio-economic benefits

According to the baseline values, the reduction or quitting of smoking is expected to generate:

- 154.03 million euros from reduction in healthcare expenditure;
- 40.53 million euros from increase in societal productivity.

Overall economic benefits

As overall quantitative results, the baseline reduction of illicit trade (30% for contraband, 10% for counterfeit, and 10% for illicit whites) is expected to generate 2.76 billion euros:

- 2.55 billion euros in revenues from an increase in legal sales;
- 204.56 million euros in other socio-economic benefits.

However, it would not be realistic to assume that all this revenue will be achieved at the very beginning of the implementation of the System. Therefore, a progressive reduction of illicit trade will be achieved over six years of System operation, concluding that the expected annualised revenues can be summarised as follows (in millions of euros):

	2018	2019	2020	2021	2022	2023	2024
Revenues from increase in legal sales	-	250.33 M€	735.68 M€	1,716.59 M€	2,201.93 M€	2,452.28 M€	2,554.45 M€
Other economic benefits	-	20.05 M€	58.91 M€	137.46 M€	176.33 M€	196.38 M€	204.56 M€
Total revenue increment	-	270.38 M€	794.59 M€	1,854.05 M€	2,378.27 M€	2,648.66 M€	2,759.01 M€

Table 16: Evolution of the economic inflows

4.3.1.2. Social and environmental benefits

Similarly, the reduction or quitting of smoking produces several social and environmental benefits to society. The main positive impact in this regard is the improvement of public health. People who do not smoke or reduce their consumption of tobacco products until eventually quitting smoking are healthier and live significantly longer. These benefits have been grouped in three categories:

- People who reduce or quit smoking
- Reduction of costs related to premature mortality due to smoking
- Other social and environmental benefits

People who reduce or quit smoking

It is possible to quantify the reduction in tobacco products consumption in terms of people. To do so, the number of people over 15 years of age in the 28 Member States has been isolated (429.1 million people), and calculated with the current smoking rate of tobacco products.

Considering an overall reduction in illicit trade of 2.45%, and that 24.85% of the current illicit tobacco purchasers would now decide to reduce their consumption or even quit smoking, the number of people who reduce or quit smoking can be modelled.

People who will reduce or quit smoking		
Total population *(Millions of people – Total EU28)*	**(H')**	**508.45**
Population above 15 years old *(Millions of people – Total EU28)*	**(I')**	**429.11**
Current smoking rate of tobacco *(Average % for EU28)*	**(J')**	**25.71%**
Number of people who will reduce or quit smoking *(Millions of people – Total EU28)*	**(K') = (P) · (S) · (I') · (J')**	**0.712**
Source: (H') (I'): (Eurostat, 2015) (J'): (Eurobarometer, 2017)		

Table 17: Summary of social benefits I

Reduction of premature mortality due to smoking

It has been demonstrated that smoking harms nearly every organ of the human body, causing a wide variety of diseases (US Department of Health and Human Services, 2004). The TPD Impact Assessment (European Commission - TPD Impact Assessment, 2012) estimates the value of one life year to be 52,000€. Therefore, the total number of life years lost per country (DG SANCO, 2008) has been reviewed in order to estimate the monetary value of life years saved by the effective implementation of the proposed measures.

Reduction of premature mortality due to smoking		
Total Life years lost (LYL) due to smoking	**(L')**	**9,936,791**
Reduction in LYL by the effective implementation of the proposed measures	**(M') = (L') · (P) · (S)**	**60,274**
Monetary value of loss ***(Millions of euros – Total EU28)***	**(N') = (M') · 52,000€**	**3,134 M€**
Source: (L'): (DG SANCO, 2008)		

Table 18: Summary of the social benefits II

Other social and environmental benefits

Others costs to society and environment related to tobacco consumption will also be reduced (ASH, 2015):

- Cost of fires caused by smokers' materials (cigarettes and other smoking materials are the primary cause of fatal accidental fires in the home);
- Improvements in the distribution chain after implementing the measures associated to the Tracking and Tracing System of tobacco products;
- Reducing illicit tobacco trade would reduce the financing of criminal groups.

4.3.2. Cost assessment

In order to analyse the full cost of the new Tracking and Tracing System within the tobacco supply chain, the total cost has been divided into five parts corresponding to the five proposed policy options:

- Governance model
- Data storage model
- Allowed data carriers
- Allowed delays in reporting events
- Method of adding a security feature

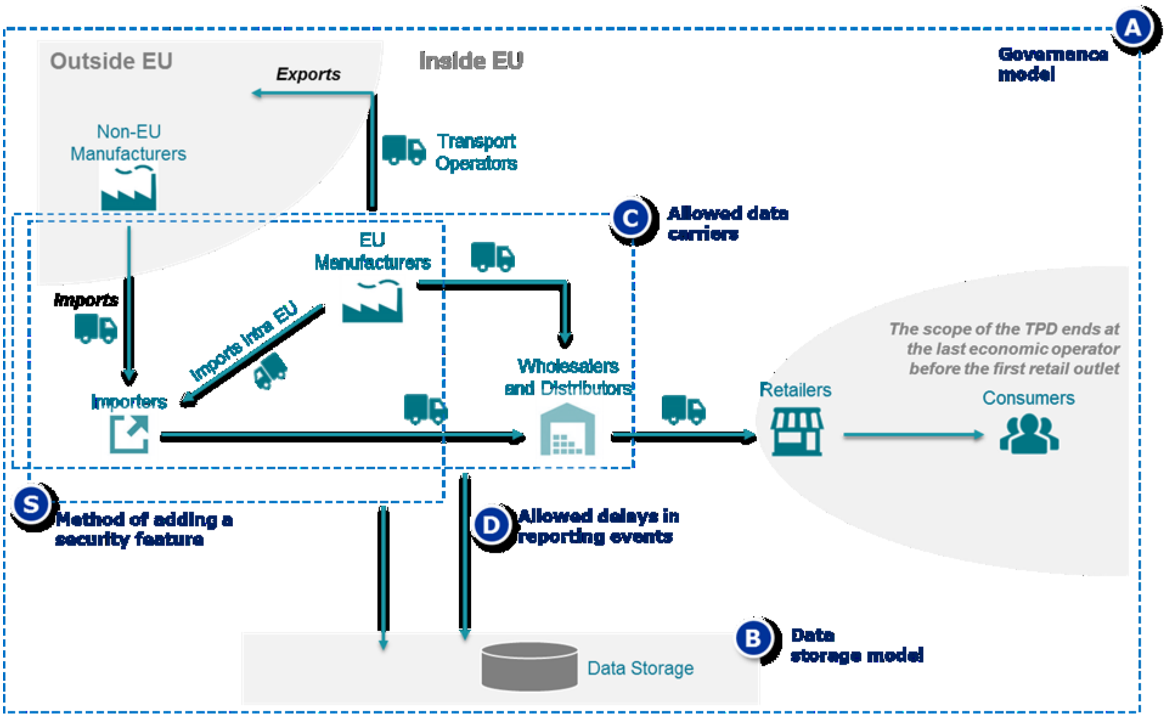


Figure 16: Tracking & Tracing System schema

The costs are distinguished between CAPEX (capital expenditures) and OPEX (operational expenditures), and they are annually distributed over a seven-year time period. Additionally, the CAPEX corresponding to the implementation of the System for cigarettes and RYO is estimated for 2018, while the CAPEX for the implementation of the System for other tobacco products is forecast for 2023. The OPEX starts as of May 2019 for tobacco and RYO and May 2024 for other tobacco products.

The detailed analysis of the cost calculation is presented in Chapter 2 of Annex I, where costs such as the data carrier generation, printing, and verifying and scanning equipment, as well as the costs related to software, hardware, communications and system auditing are identified. The following table summarises the annualised costs split by typology and policy option.

	2018	2019	2020	2021	2022	2023	2024
CAPEX - Governance model	92.56	-	-	-	-	3.78	-
CAPEX - Data storage model	18.26	-	-	-	-	0.75	-
CAPEX - Allowed data carriers	160.98	-	-	-	-	6.59	-
CAPEX - Allowed delays in reporting events	37.45	-	-	-	-	1.53	-
CAPEX - Method of adding a security feature	-	-	-	-	-	-	-
CAPEX - TOTAL	309.26	-	-	-	-	12.65	-
OPEX - Governance model	-	17.25	25.88	25.88	25.88	25.88	26.58
OPEX - Data storage model	-	4.66	7.00	7.00	7.00	7.00	7.19
OPEX - Allowed data carriers	-	6.18	9.28	9.28	9.28	9.28	9.53
OPEX - Allowed delays in reporting events	-	27.00	40.51	40.51	40.51	40.51	41.61

	2018	2019	2020	2021	2022	2023	2024
OPEX - Method of adding a security feature	-	9.53	14.30	14.30	14.30	14.30	14.69
OPEX - TOTAL	-	64.64[8]	96.97	96.97	96.97	96.97	99.61

Table 19: Detailed CAPEX and OPEX (Millions of euros) - Interim Report II

4.3.3. Evaluation

The costs of the system are considerable, but it is important to notice that the solution has the potential to generate a large amount of revenue for Member States, economic operators, and EU citizens.

The following figure shows the combination of revenues and costs previously calculated.

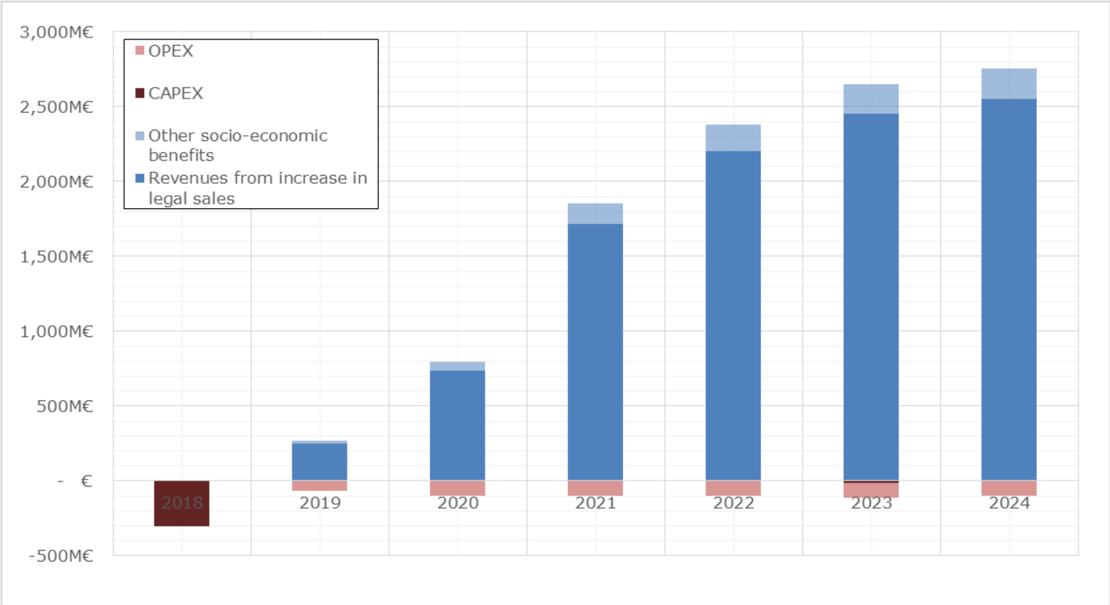


Figure 17: Comparison between the revenues and the costs of the solution (million €)

In our model, the expected revenues largely surpass the expected costs of implementing the System (CAPEX) and the recurrent costs of operating it (OPEX). The revenues are quantified in terms of revenues from the increase in legal sales (new tax revenues and new revenues for economic operators involved in the value chain of tobacco products) and other socio-economic revenues (lower health care spending and new revenues from increased productivity).

These values are based on a set of assumptions and lack real-life testing, but they are an important baseline to evaluate the implementation of the solution. Many other studies (Reed, 2010) (Joossens, Merriman, Ross, & Raw, 2010) reinforce the idea that the revenues of implementing systems that help to eliminate global illicit trade surpass the costs of the implementation of such systems.

[8] The OPEX for 2019 are influenced by the fact that the measure becomes effective in May of that year.

Some deviations can occur when implementing the solution, but it is equally true that economies of scale can be attained that may reduce some of the costs modelled. In the end, the solution has the potential to generate considerable benefits over the years, even if the economic operators must make a large initial investment.

5. Technical specifications for the Tracking and Tracing System

The Tracking and Tracing System can be understood as the interaction between the physical flow and the information flow, and can be divided into three major conceptual domain groups:

- **Supply Chain**: the domain where merchandise is traded;
- **IT**: the domain that interacts with information, further divided into:
  - **UI Generation**: the domain where the unique identifier is generated.
  - **Data Storage**: the domain where the data is stored.
- **Surveillance**: the domain where competent authorities and auditors access data.

An overview of the Tracking and Tracing System is depicted in the diagram below:

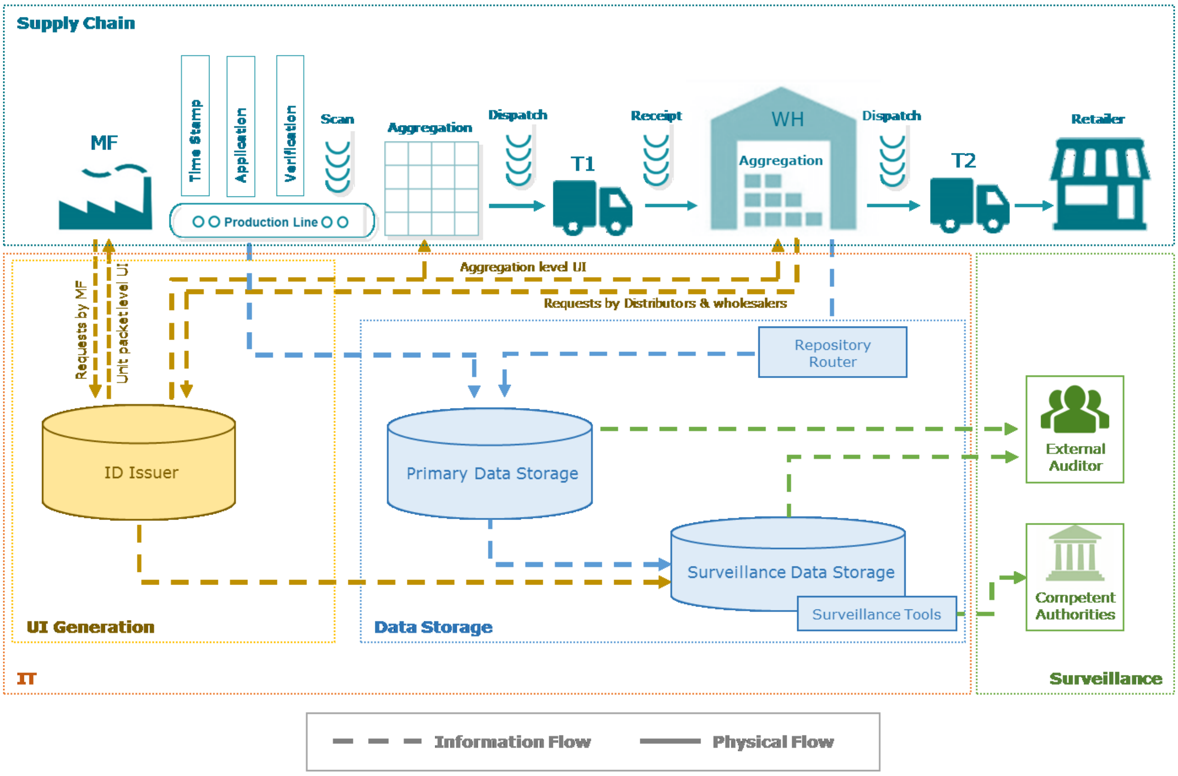


Figure 18: System overview diagram

The next subsections include the detailed definition and explanation of the elements included in the supply chain and IT domains.

5.1. Supply chain elements

The supply chain domain categorises economic operators according to their production and movement of tobacco products throughout the supply chain. The tracking and tracing events belonging to this domain are: scanning, aggregation, dispatch, and receipt of unique identifiers. The details of the supply chain processes are presented in Section 1.3 of Annex II: *"Business Process Diagrams"*.

This subchapter on the technical specifications for the Tracking and Tracing System aims to provide an assessment regarding the following elements:

- Unique identifiers (at unit packet / aggregation packaging level): Provides an assessment of the requirements, composition, authentication and procedures for deactivation of the unique identifier together with the description of the generation of serial numbers and rules for aggregation.
- Data carrier (at unit packet / aggregation packaging level): Describes the most commonly used and up-to-date data carriers, industry constraints, authorised data carriers, rules for placement, and technical requirements.
- Anti-tampering system: Describes the devices or processes that make unauthorised access to the specific stages of the manufacturing process easily detected.

Furthermore, Chapter 2 of Annex II*: "Detailed technical specifications for the supply chain elements of the tracking and tracing system"* further develops the topics contained in the table below:

Subsection	Content
2.1	Unique identifier at unit packet level
2.2	Unique identifier at aggregation packaging level
2.3	Data carrier at unit packet level
2.4	Data carrier at aggregation packaging level

Table 20: Annex II – Chapter 2: Detailed technical specifications for the supply chain elements of the Tracking and Tracing System

5.1.1. Unique identifier (at unit packet level)

5.1.1.1. Composition of the unique identifier at unit packet level

The Article 15(1) of the TPD requires all unit packets of tobacco products to be marked with a unique identifier. Additionally, Articles 15(2) and 15(3) require that the following elements form part of the unique identifier:

TPD Article	TPD Request
15(2a)	Date of manufacturing
15(2a)	Place of manufacturing
15(2b)	Manufacturing facility
15(2c)	Machine used to manufacture the tobacco products
15(2d)	Production shift or time of manufacture
15(2e)	Product description
15(2f)	Intended market of retail sale
15(2g)	Intended shipment route
15(2h)	Where applicable, the importer into the union

Table 21: Directive 2014/40/EU requirements

Ensuring that the nine above-mentioned data elements form part of the unique identifier poses certain challenges:

- **Length of the unique identifier**. It is necessary to include a high number of data elements in the unique identifier. The optimal size of the unique identifier to be applied to a unit packet of tobacco products should not exceed 60 characters and preferably be closer to 40 characters[9]. Otherwise, the negative impact on high-speed production lines is likely to be significant.
- **Access to readable information** for competent authorities. However, the data elements that form part of the unique identifier can be previously encoded to reduce the length of the unique identifier. This suggests that use could be made of lookup tables as an instrument to decode and convert the codes into readable information for competent authorities, thereby increasing the effectiveness of surveillance activities.

Consequently, the study conducts a three-step analysis to propose an optimal coding format for the unique identifier, which is capable of complying with the requirements of the TPD and minimising the impact on the printing equipment of the production lines (see Annex II – Chapter 2*: Detailed technical specifications for the supply chain elements of the Tracking and Tracing System*).

The steps of this analysis are:

1. **Information analysis** to identify the different attributes that qualify and categorise the information.
2. **Grouping of data elements** to promote possible data relationships and synergies.
3. **Sizing optimization** to reduce the length of the unique identifier.

Structure of the unique identifier

The three-step analysis undertaken by the Implementation Study suggests a 34 alphanumeric-digit unique identifier formed by four information elements according to the nature of their generation: ID Issuer identification code, serial number, primary information (place of manufacture, manufacturing facility, machine used to manufacture the tobacco products, product description, intended market of retail sale, intended shipment route and where applicable, the importer into the EU) and secondary information (manufacturing timestamp), thereby encoding the nine data elements required to form part of the unique identifier by Article 15 .

Element ID	Information requested	TPD Reference	Code example	Length estimation
UID_1 ***ID Issuer***	**ID Issuer identification**		A3	2

[9] The unique identifier's length negatively impacts the production speed rate since the requested data carriers need longer production times to be printed

Element ID	Information requested	TPD Reference	Code example	Length estimation
identification				
UID_2 ***Serial number***	**Serial number**		AAE5F46G7H	10
UID_3 ***Primary information***	**Place** of manufacture	Art 15(2)(a)	A1B2C3D4L2M3N4	14
	Manufacturing **facility**	Art 15(2)(b)		
	Machine used to manufacture the tobacco products	Art 15(2)(c)		
	Product description	Art 15(2)(e)		
	Intended **market** of retail sale	Art 15(2)(f)		
	Intended shipment **route**	Art 15(2)(g)		
	Where applicable, the **importer** into the EU	Art 15(2)(h)		
UID_4 ***Secondary information***	Manufacturing **timestamp** (Date of manufacture and time of manufacture or production shift)	Art 15(2)(a) Art 15(2)(d)	21043013	8
Total				**34**

Table 22: Structure of the unique identifier at unit packet level

Consequently, some of the unique identifier's data elements would require the establishment of lookup tables. Lookup tables are tools that enable users to encode a certain volume of information into a more compact and secure format by using codes as identifiers (see Annex II – Chapter 2*: Detailed technical specifications for the supply chain elements of the Tracking and Tracing System*). The following table summarises the estimated size of the required lookup tables.

Information requested	Realistic size	Maximum size
Location of the manufacturing activities	19.13Mb	359Mb
Product description	11.64Mb	242Mb
Intended **market** of retail sale	19.3Kb	2Mb
Intended shipment **route**		
Where applicable, the **importer** into the EU	134Kb	6.71Mb

Table 23: Summary of the lookup table's size

The unique identifier should be structured by four information elements sorted as follow:

1. **ID Issuer identifier**.

   - The identification code of the independent ID Issuer responsible for providing the serial numbers.

2. **Serial number**, generated by an independent ID Issuer.
   - The combination of the primary information, ID Issuer identification code and the serial number guarantees the code's uniqueness for each unit packet.
3. **Primary information**, required by the ID Issuer from the manufacturer or importer.
   - Formed by seven data elements: place of manufacturing, manufacturing facility, machine, product description, intended market information, shipment route information and, where applicable, importer.
4. **Secondary information**, included by the manufacturer.
   - Formed by one element of information: manufacturing timestamp.

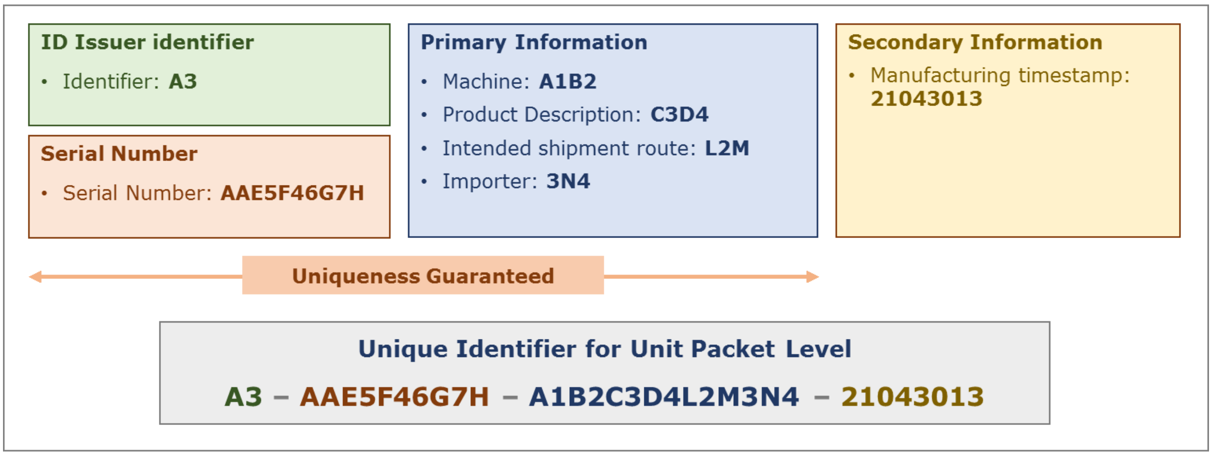


Figure 19: Composition of the unique identifier at unit packet level

5.1.1.2. Generation of serial numbers at unit packet level

The generation of serial numbers shall be done by an independent third party provider (ID Issuer) upon the request of the economic operators. Several ID Issuer solutions can be established by independent third parties in order to promote fair and open competition at EU level, and encourage the decentralised framework intended and prescribed by the European Union legislature.

The generation of serial numbers is further described in the points below.

- Production needs shall not be predictable through the assignment of non-sequential serial numbers. Thus, the ID Issuer shall avoid allocating sequential numbers or predefined ranges of serial numbers.
- The economic operators shall request a batch of serial numbers according to their needs through a secure interface published by the ID Issuer solution.
- The generation flow is as follows:

- The economic operator issues a remote request, providing the primary information and the number of serial numbers requested.
- The system verifies the sender authenticity and the information provided within his/her request.
- The batch of serial numbers is generated according the following rules:
  - Each serial number is non-sequential.
  - The probability of guessing a serial number is negligible.
  - The ID Issuer stores the serial numbers that have been generated in order to avoid duplications.
- The ID Issuer notifies the Primary Data Storage, via the router, of the parts of the unique identifiers it has generated: i.e. the batch of serial numbers, the ID issuer identification code and the encoded primary information.

The relationships between the actors and systems involved in the generation of serial numbers are depicted below:

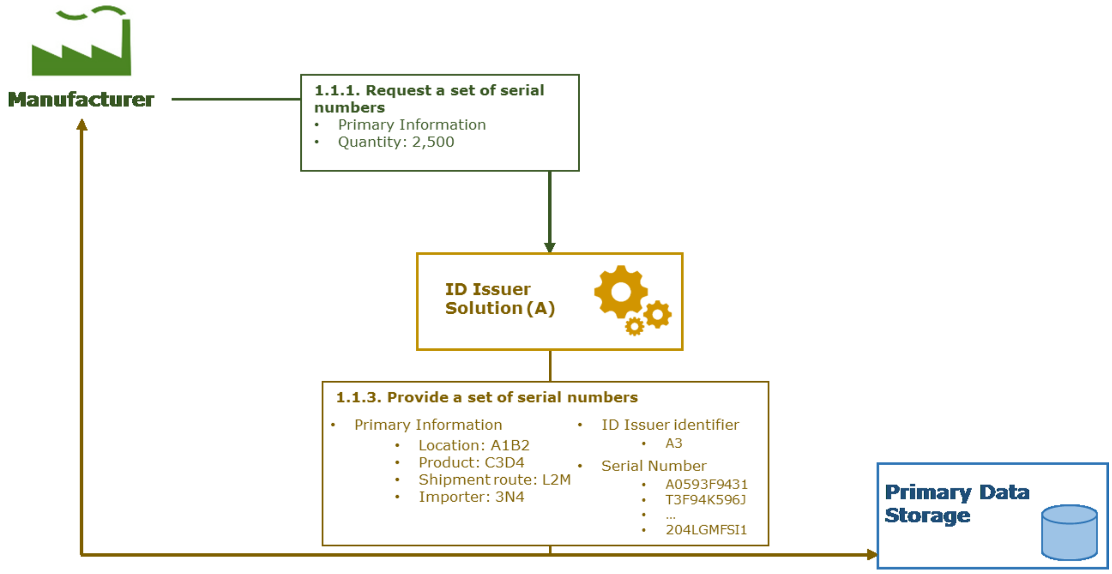


Figure 20: Generation of serial numbers – global view

5.1.1.3. Unique identifier authentication

Unique identifier authentication is the process of verifying the readability of the data carrier and the authenticity of the unique identifier read.

Once the unique identifier is created, the information is transmitted to the printing equipment that encodes it in a data carrier and prints or affixes it to the unit packet. Then the unit packet goes through the verification process, which performs the following two activities:

1. **Verification**. If the data carrier cannot be read, the unit packet has to be repackaged.
2. **Transmission**. If the data carrier is readable, the information contained is decoded and transmitted to the Primary Data Storage (and later to the

Surveillance Data Storage) where it will be compared with the information previously received by the ID Issuer to verify its authenticity.

The conceptual process of the unique identifier printing and verifying is shown in the figure below:

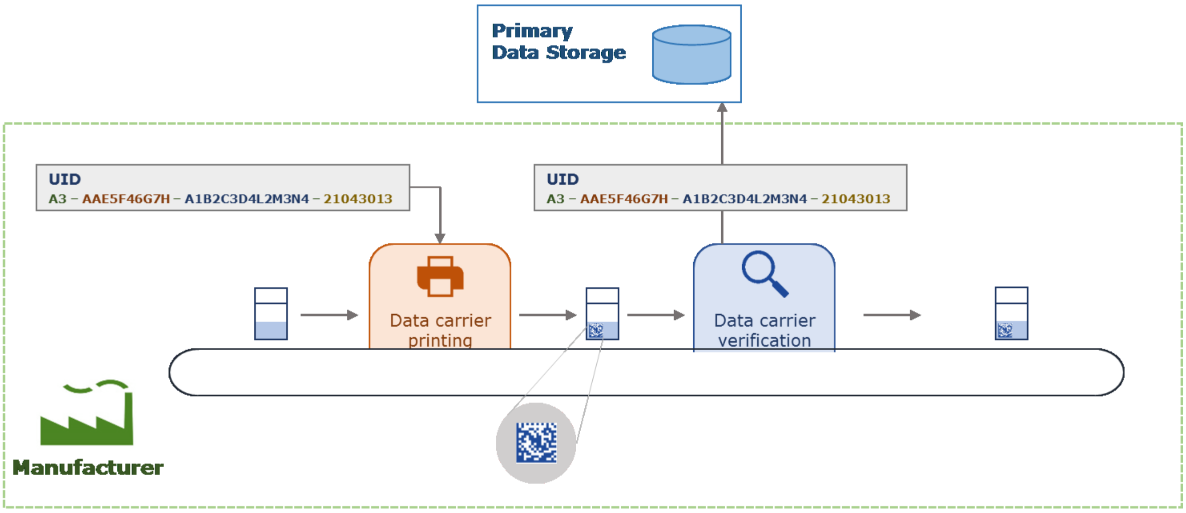


Figure 21: Unique identifier authentication at unit packet level

The Surveillance Data Storage keeps record of all the unique identifiers retrieved by the ID Issuers. These unique identifiers remain in the Surveillance Data Storage under the status "Generated" until a specific event trigger the change of their status. The unique identifier status can evolve from "Generated" to three different statuses:

- Activated: The unique identifier, after being transmitted by the manufacturer, matches a unique identifier stored in the Surveillance Data Storage under the status "Generated". Additionally, the information contained in the secondary information (date and time of manufacture) matches the valid activation date for that unique identifier.
- Deactivated: The manufacturer reports the deactivation of that unique identifier. Another reason for deactivation may be that a manufacturer has tried to activate a unique identifier whose secondary information (date and time of manufacture) does not match the valid activation date for that unique identifier.
- Expired: The valid activation date expires for the unique identifier. In this case, the Surveillance Data Storage automatically performs this change of status.

5.1.1.4. Unique identifier deactivation

The causes for deactivating a unique identifier can be multiple, from damage to the unit packet, to quality problems in the production line, to decisions to remove a product from the market.

- **Primary Data Storage notification**: The economic operator responsible must report the deactivation to the Primary Data Storage. This deactivation message is formed by components including the economic operator, the unique identification of the unit packet and the cause of deactivation.

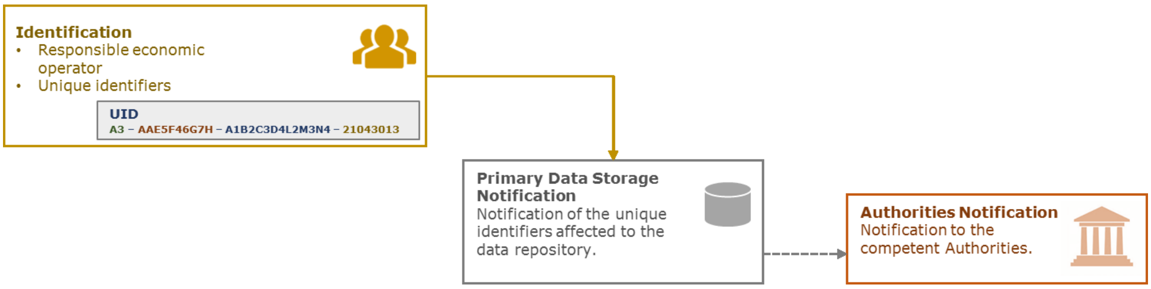


Figure 22: Process for deactivation at unit packet level

5.1.2. Unique identifier (at aggregation packaging level)

5.1.2.1. Composition of the unique identifier at aggregation packaging level

Article 15(5) of the TPD sets out that the traceability requirements may be complied with by the marking and recording of aggregation packages such as cartons, mastercases or pallets. Aggregation packages should be marked with a unique identifier to facilitate the activities of the Tracking and Tracing System, allowing an increase in operational efficiency while reducing costs in the supply chain.

In order to do so:

- The identification of the aggregation packages must be unique;
- The unique identifier at aggregation packet level must be linked with the unique identifiers of the elements contained inside.

Nevertheless, unique identifier creation implies certain challenges:

- **Length of the unique identifier**. 1D data carriers are widely used in distribution chain operations. In order to be able to use a variety of data carrier types, the length of the unique identifier should not exceed a certain number of characters.
- **Access to readable information** for competent authorities. As previously stated, readable information is necessary to maximise the potential of the competent authorities to reduce illicit trade.

Therefore, a two-step analysis has been conducted to propose the most optimal coding format for the unique identifier, while complying with the requirements of the TPD and minimising the impact on the printing equipment of the production lines at aggregation packaging levels (see Annex II- Chapter 2*: Detailed technical specifications for the supply chain elements of the Tracking and Tracing System*). The two steps or this analysis are:

1. **Information analysis:** to identify the different attributes that qualify and categorise the information.
2. **Sizing optimization:** to reduce the length of the unique identifier.

Structure of the unique identifier

The two-step analysis under taken by the Implementation Study suggests a 24 alphanumeric digit code that assures uniqueness and is formed by four information elements: ID Issuer identification code, Serial number, Primary information and Secondary information.

Element ID	Information provided	Code example	Length estimation
UID_1 ***ID Issuer identification***	**ID Issuer identification**	A3	2
UID_2 ***Serial number***	**Serial number**	T03K55E322	10
UID_3 ***Primary information***	**Location** of the aggregation activities	A5R2	4
UID_4 ***Secondary information***	Aggregation activities **timestamp**	21043013	8
Total			**24**

Table 24: Example of location of manufacturing activities code

Moreover, one element requires the establishment of lookup tables, which could be merged with the unit packet level to reduce the complexity of the system.

Element ID	Information requested	Realistic size	Maximum size
UID_1	**Location** of the manufacturing or aggregation activities	19.13Mb	359Mb

Table 25: Summary of lookup tables size

The unique identifier at aggregation packaging level should be structured by four information elements sorted as follows:

1. **ID Issuer identifier**.
   - The identification code of the independent ID Issuer responsible for providing the serial numbers.
2. **Serial number**, generated by an independent ID Issuer.
   - The combination of the primary information, ID Issuer identification code and the serial number guarantees the code’s uniqueness for each aggregation packaging.
3. **Primary information**, required by the ID Issuer from the economic operator.
   - Formed by one element of information: location of the aggregation activities.
4. **Secondary information**, included by the economic operator.
   - Formed by one element of information: aggregation activities timestamp.

Figure 23: Composition of the unique identifier at aggregation packaging level

5.1.2.2. Generation of serial numbers at aggregation packaging level

The generation of serial numbers for the unique identifier at aggregation packaging level shall be done by an ID Issuer. The ID Issuer shall be an independent third party provider, responsible for generating serial numbers according to specific rules. The ID Issuer generates the serial numbers at economic operators' request. Several ID Issuer solutions may be established by independent third parties in order to promote fair and open competition at EU level, and encourage the decentralised framework intended and prescribed by European Union legislature.

The generation of serial numbers at aggregation packaging level is further described in the points below.

- Production needs shall not be predictable through the serial number. Thus, the ID Issuer shall avoid allocating sequential numbers or predefined ranges of serial numbers.
- An interface is published where the economic operators request a batch of serial numbers according to their needs.
- The generation flow is as follows:
  - The economic operator issues a remote request comprising the primary information and the number of serial numbers requested:
  - The solution verifies the sender authenticity and the information provided within his request.
  - The set of serial numbers is generated according the following rules:
    - Each serial number is non-sequential.
    - The probability of guessing a serial number is negligible.
    - The ID Issuer stores the serial numbers that have been generated in order to avoid duplications.
  - The ID Issuer notifies the Primary Data Storage (in the case of manufacturers and importers) or the Surveillance Data Storage (in the case of other economic operators) of the parts of the aggregation packaging level unique identifiers it has generated: i.e. the batch of serial

numbers, the ID issuer identification code and the encoded primary information.

The relationships between the users and systems involved in the generation of serial numbers are depicted below:

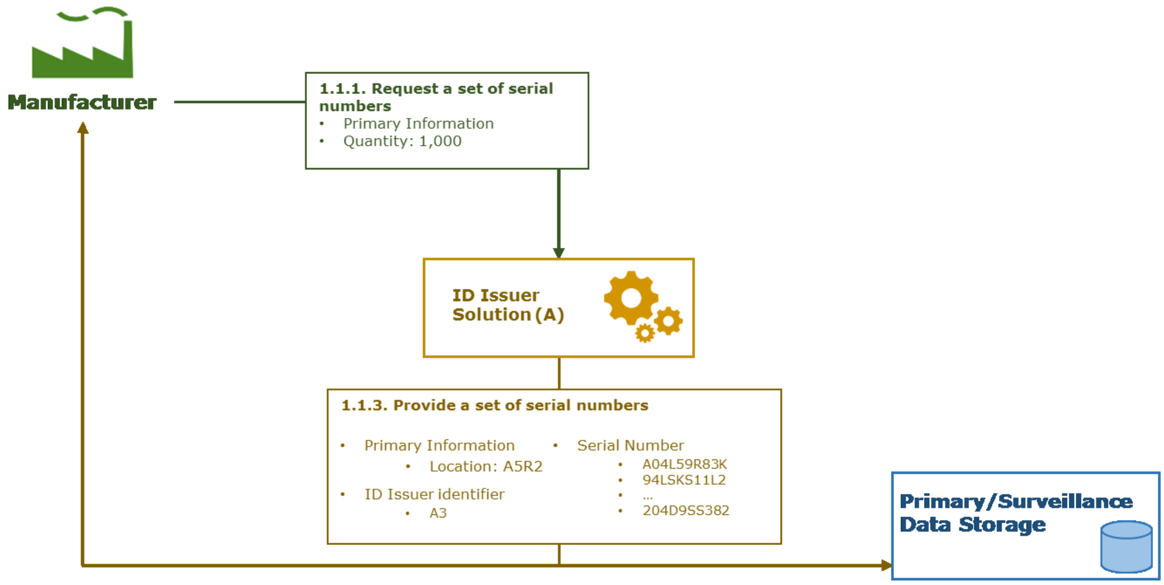


Figure 24: Generation of serial numbers – global view

5.1.2.3. Rules for aggregation and deactivation

Procedure for aggregation and unique identifier authentication

The aggregation of tobacco products is used to establish relationships between different packaging units, permitting their traceability along the supply chain while improving the effectiveness of operational processes.

In order to do so, the items within a container (carton, master case, pallet, etc.) are recorded, and a unique identifier is assigned to the container. Then, the unique identifier on the container can be used as a basis to record the movement of the container (with its contents) through the distribution chain.

Hence, this hierarchy enables linking unit packets with cartons, cartons with master cases and master cases with pallets. This union is outlined in the following figure, where ten unique identifiers at unit packet level are linked with one unique identifier at carton level.

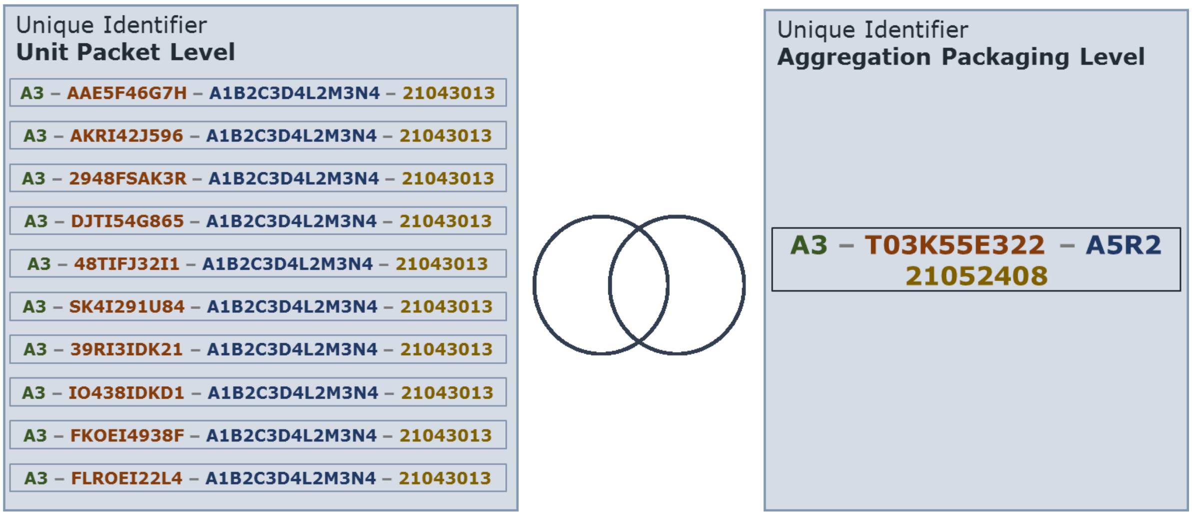


Figure 25: Link between unique identifiers at different levels of aggregation

Aggregation processes can take place in manufacturer and importer facilities, but also in distribution chain operator facilities, requiring the following sub-processes:

1. **Identify** all the unique identifiers of the items to be contained in the container.
2. **Generate** the unique identifier for the aggregation package and print or affix the data carrier.
3. **Verify** the readability of the data carrier. If the data carrier cannot be read (i.e. it has not been correctly printed), the verifying equipment sends the aggregation packaging to be repackaged.
4. **Link** to the database for the unique identifiers of the contained items with the unique identifier of the container.

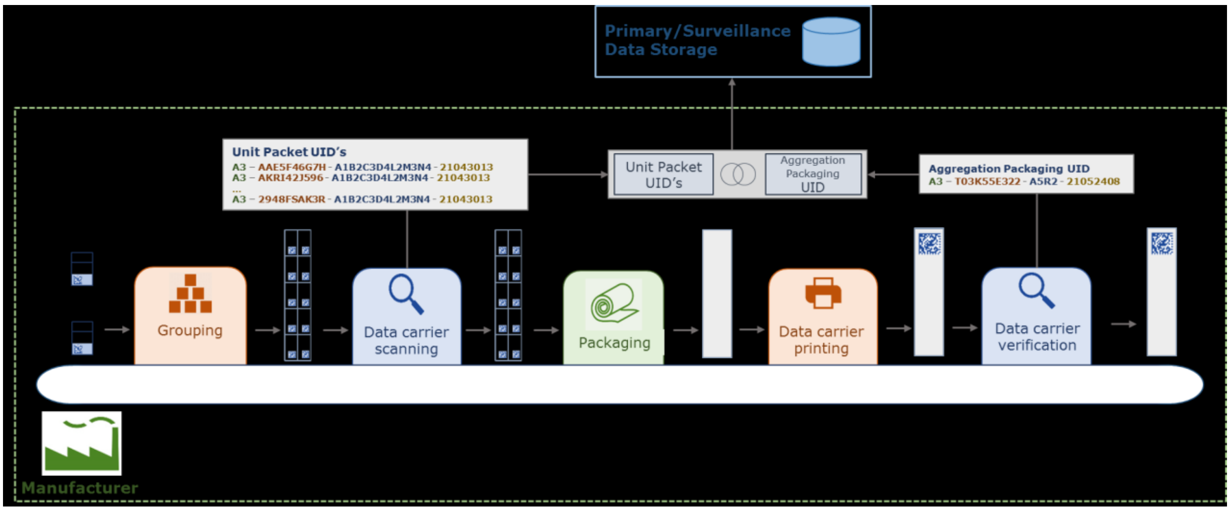


Figure 26: Aggregation processes and linkage of unique identifiers

The Surveillance Data Storage keeps record of all the unique identifiers for aggregation packaging retrieved by the ID Issuers. These unique identifiers remain in the Surveillance Data Storage under the status "Generated" until a specific event triggers the changing of their status. The unique identifier's status can evolve from "Generated" to three different statuses:

- Activated: The unique identifier, after being verified by the aggregator, matches a unique identifier stored in the Surveillance Data Storage under the status "Generated". Additionally, the information contained in the secondary information matches the valid activation date for that unique identifier.
- Deactivated: The aggregator reports the deactivation of that unique identifier. Another cause of deactivation is when an aggregator tries to activate a unique identifier whose secondary information does not match the valid activation date for that unique identifier.
- Expired: The valid activation date expires for that unique identifier. In this case, the Surveillance Data Storage automatically performs the change of status.

Procedures for deactivation

The causes for deactivating a unique identifier can vary, from damage to the aggregation package, to quality problems in the production line.

Primary/Surveillance Data Storage notification: The economic operator responsible must report the deactivation to the Primary Data Storage (in the case of manufacturers and importers) or to the Surveillance Data Storage (in the case of other economic operators). This deactivation message is formed by components including the economic operator, the unique identification of the unit packet and the cause of deactivation.

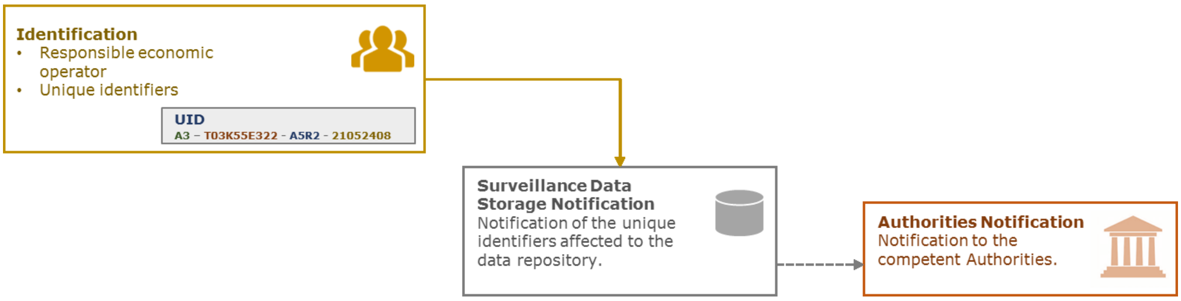


Figure 27: Process for deactivation at aggregation packaging level

5.1.3. Data carrier (at unit packet level)

5.1.3.1. Competitive landscape analysis

The purpose of the competitive landscape analysis is to identify the variety of data carriers that could include the unique identifier without altering the feasibility of operation. The selected variety of data carriers must fulfil the following requirements, which are related to the ability to include the unique identifier, the ability to freely use the data carrier, and the high degree of industry adoption.

- The data carrier allows encoding alphanumeric digits.
- The maximum number of characters enabled in the data carrier is higher than the current length of the unique identifier (34 characters).
- The data carrier is not restricted to specific industries or organisations.

- The code specifically represents a data carrier symbology.
- The data carrier is already implemented in the operations of manufacturers, importers and distributors.

The table below presents the variety of data carriers that fulfil the previously stated requirements. (Priyanka Gaur, 2014) (GS1, 2015) (TEC-IT, 2017) (University, 2011) (Cognex, 2013).

Data Carrier	Description	Example
Code 128	• 1 Dimensional data carrier. • It can encode all 128 characters of ASCII. • The symbology is defined as ISO/IEC 15417:2007.	
Aztec Code	• 2 Dimensional data carrier. • All 8-bit values can be encoded. • It has the potential to use less space than other matrix barcodes. • The symbology is defined as ISO/IEC 24778:2008.	
Data Matrix	• 2 Dimensional data carrier. • It can encode the entire ASCII character set. • It can include up to 2,335 alphanumeric characters. • The symbology is defined as ISO/IEC 16022:2006.	
DotCode	• 2 Dimensional data carrier. • It can encode ASCII characters. • It is ideally suited for high speed industrial ink jet and laser marking techniques. • DotCode symbology specifications are defined by AIM.	
QR	• 2 Dimensional data carrier. • It can encode the entire ASCII character set. • It can include up to 4,296 alphanumeric characters. • The symbology is defined as ISO/IEC 18004:2006.	
PDF417	• It is a stacked linear data carrier. • It can encode all 128 characters of ASCII. • The symbology is defined as ISO/IEC 15438:2006.	

Table 26: Preliminary selection of data carriers

5.1.3.2. Industry constraints and evaluation parameters

The final stage of the project implementation takes place at a shop floor level, where manufacturing operations deal with the data carriers proposed to include the unique identifier.

Industry constraints

In order to facilitate the selection of the most adequate data carriers, the implementation team has reviewed the manufacturing characteristics for the different types of tobacco products and their distribution processes. Consequently, the following insights are highlighted:

- Manufacturer and importer constraints:
    - Grand variety of SKUs and different varieties of tobacco products
    - Production line speed

- Size and shape of the different SKUs
- Packaging materials

- Distribution chain operator constraints:
    - Ability to scan the selected data carriers

The review of the feedback from the Stakeholder Consultation and the visits of the implementation team to several manufacturing plants highlights the differences in the printing processes for several sets of products. Four different categories of manufacturing characteristics, influenced by two main drivers – the production speed (high-speed production vs low/medium-speed production) and the product type (cigarettes vs other tobacco products) – are selected as representatives of the printing conditions for the wide spectrum of tobacco products. These are represented in the following matrix:

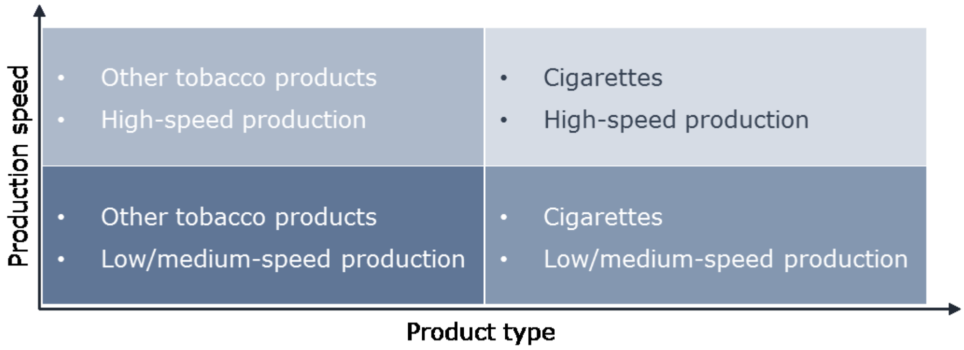


Figure 28: Product type vs production speed matrix

Evaluation parameters

Therefore, a criteria analysis is conducted in order to find the data carrier that best adapts to the traceability operations for each set of items. The study scores the performance of each selected data carrier for the criteria and appoints the best data carrier to contain the unique identifier for each product category.

Three major evaluation parameters have been identified:

1. Technical feasibility
    - Ability to adapt the data carrier to the unit packet of all tobacco products
    - Impact generated by the printing or affixing activities on the manufacturer and importer production processes
    - Availability of different suppliers
    - Ability to adapt to quality control activities
2. Operational requirements
    - Adaptability of printing and verifying activities to production lines
3. Burden on stakeholders
    - Burden of registration activities
    - Cost of printing and verifying equipment for manufacturers
    - On-going cost of printing and verifying activities

5.1.3.3. Allowed data carriers

The objective of the criteria analysis was to select the type of data carrier that best suits the needs of each of the categories highlighted (see Annex II- Chapter 2*: Detailed technical specifications for the supply chain elements of the Tracking and Tracing System*). The analysis pinpoints three data carriers - Data Matrix, DotCode and QR – as the most suitable to contain the unique identifier at unit packet level.

Each unit packet of any tobacco product should be marked with one of these data carriers. The following table contains their main characteristics.

Data Carrier	Characteristics	Example
Data Matrix	• Able to be printed by multiple technologies either directly on the package or on a label to later be affixed. • Currently used in the marking of tobacco products other than cigarettes.	
DotCode	• Able to be printed in high-speed production lines through continuous ink jet or laser printing technologies. • Currently used at unit packet level by several tobacco manufacturers.	
QR	• Able to be printed by multiple technologies either directly on the package or on a label to later be affixed. • It is one of the most used data carriers worldwide and compatible with multiple scanning solutions.	

Table 27: Allowed data carriers for unit packet of tobacco products

5.1.3.4. Human-readable interpretation

The human-readable interpretation refers to the set of characters, such as letters or numbers, which can be read by any user with the aim of decoding the unique identifier without scanners.

Although the TPD does not request the addition of this code, the study proposes it as a complementary measure to increase the robustness of the System. This code is particularly useful in situations where the data carrier has been damaged or when stakeholders do not possess the equipment to correctly read the data carrier, and can prevent potential disruptions in the supply chain. Nevertheless, the circulation of unit packets in the supply chain with illegible data carriers should not be permitted. In these situations, human-readable codes will be especially useful to proceed with the deactivation process.

A human-readable code is especially useful when reaching the final customer, because it permits the future establishment of a use case where the authenticity and traceability of a single unit packet can be verified.

The human-readable code should comply with the following:

- Contain the information elements that enable identification of the unique identifier.

- Its length should allow flexibility of operation and should not increase the complexity of the printing process.

The uniqueness of the code is guaranteed by combining the primary information (place of manufacture, facility, machine, product description, intended market and shipment route information and importer), the ID Issuer identification code and the serial number. Consequently, the Implementation Study proposes the following:

- The human-readable code is comprised of three information elements:
    - The first code contains the ID Issuer identification code (2 characters).
    - The second code contains the serial number (10 characters).
    - The third code contains the primary information (14 characters).

Consequently, the human-readable code is printed along with the data carrier. It distinguishes the groups of information by separating them with a "dash" character or a "line break".

A3 – AAE5F46G7H
A1B2C3D4L2M3N4

A3 – AAE5F46G7H
A1B2C3D4L2M3N4

A3 – AAE5F46G7H
A1B2C3D4L2M3N4

Figure 29: Examples of human-readable codes associated to data carriers

5.1.4. Data carrier (at aggregation packaging level)

5.1.4.1. Competitive landscape analysis

The competitive landscape analysis identifies the variety of data carriers that could include the unique identifier at aggregation packaging level, while complying with a set of requirements. These data carriers shall be able to include the data, be used without restrictions, and offer ease of industry adoption.

- The data carrier allows encoding alphanumeric digits.
- The maximum number of characters enabled is higher than the length of the unique identifier (24 characters).
- The data carrier is not restricted to specific industries or organisations.
- The code represents specifically a data carrier symbology.
- The data carrier is already implemented in the manufacturing, importing and distributing operations.

The selected variety of data carriers coincides with that presented in Section 5.1.3 for unit packet level. They are: Aztec Code, Code 128, Data Matrix, DotCode, QR Code and PDF417.

5.1.4.2. Industry constraints and evaluation parameters

Industry constraints

The assessment of the most appropriate data carriers to contain the unique identifier at aggregation packaging level is based on a review of the manufacturing and distribution activities for the different tobacco products. In this study, the implementation team has identified the following indicators as relevant in the selection of data carriers:

- Manufacturers and importers constraints:
    - Different levels of aggregation
    - Production line speed
    - Size and shape of the different SKUs
    - Materials of the packages
- Distribution chain operators constraints:
    - Ability of the distribution chain operators to read the codes

The review of the Stakeholders Consultation and the visits of the implementation team to several manufacturing plants highlighted the differences in the printing processes for several product sets.

Two different categories have been identified as representative of the aggregation packaging levels, differentiated by level of aggregation.

Figure 30: Levels of aggregation of tobacco products

Evaluation parameters

A criteria analysis was conducted in order to identify the data carrier that is most able to adapt to the traceability operations for each set of items. This analysis scored the performance of each selected data carrier against the evaluation parameters listed below and appointed the best data carrier to contain the unique identifier for each product category.

Three major evaluation parameters were identified:

1. Technical feasibility
    - Ability to adapt the data carrier to the aggregation packaging of all tobacco products
    - Impact generated by the printing or affixing activities on the production processes of manufacturers and importers
    - Feasibility of implementing data carrier reading devices for wholesalers and distributors
    - Availability of different suppliers
    - Ability to adapt to quality control activities
2. Operational requirements

- Adaptability of printing and verifying activities to production lines
- Adaptability of scanning activities to stakeholder operations

3. Burden for stakeholders
   - Burden of registration activities
   - Cost of printing and verifying equipment for manufacturers
   - Cost of scanners for distribution chain operators
   - On-going cost due to printing and verifying activities

5.1.4.3. Allowed data carriers

The criteria analysis selected the types of data carrier that best address the requirements for each highlighted category (see Annex II- Chapter 2*: Detailed technical specifications for the supply chain elements of the Tracking and Tracing System*). The analysis identified three data carriers - Data Matrix, Code 128 and QR – as the most suitable to hold the unique identifier at aggregation packaging level.

Data Carrier	Characteristics	Example
Data Matrix	• Able to be printed by multiple technologies, either directly on the package or on a label to later be affixed. • Currently used in the marking of aggregation packaging of tobacco products.	
Code 128	• Widely used in logistics operations and readable by laser scanners. • Currently used in the marking of aggregation packaging of tobacco products.	
QR	• Able to be printed by multiple technologies either directly on the package or on a label to later be affixed. • It is one of the most used data carriers worldwide and compatible with multiple scanning solutions.	

Table 28: Allowed data carriers for aggregation packaging levels of tobacco products

5.1.4.4. Human-readable interpretation

As stated in section 5.1.3.4. the human-readable interpretation refers to the set of characters, such as letters or numbers, which can be read by any user with the aim of decoding the unique identifier without scanners. Although the TPD does not request the addition of this code, the study proposes it as a complementary measure to increase the robustness of the System.

The uniqueness of the code is guaranteed by combining the primary information (location of the aggregation activities), the ID Issuer identification code and the serial number. Consequently, the Implementation Study proposes the following:

- The human-readable code is comprised of three information elements:
  - The first code contains the ID Issuer identification code (2 characters).
  - The second code contains the serial number (10 characters).

  - The third code contains the primary information (4 characters).

Consequently, the human-readable code is printed along with the data carrier. It distinguishes the groups of information by separating them with a "dash" character or a "line break".

A3 – T03K55E322 – A5R2

A3 – T03K55E322
A5R2

A3 – T03K55E322
A5R2

Figure 31: Examples of human-readable codes associated to data carriers

5.1.5. Anti-tampering system

5.1.5.1. Concept and review of the affected processes

If manufacturers and importers are to be responsible for ensuring the application of unique identifiers at unit packet level, the Implementation Study proposes the use of an anti-tampering system to protect the process of verification of unique identifiers. The anti-tampering system is a selection of devices or processes that controls and facilitates the detection of unauthorised access to, or interference with, the protected object.

In order to ensure system independence, control over the process of verifying the data carriers applied to unit packets should be ensured. This report therefore describes and proposes an anti-tampering system, which should, as a minimum, entail:

- That the anti-tampering system is operated by an external third party approved by the competent authorities with the objective of increasing their control of the system and assisting them in identifying all potential or suspected cases of unauthorised interference/tampering;
- And as optional additional features the anti-tampering system could:
  - Improve the tamper resistance by making tampering more difficult, time-consuming, etc.;
  - Add tamper-evident features to help indicate the existence of tampering.
  - Inform of the occurrence of unauthorised tampering activities in the manufacturing lines of tobacco products by verifying the legitimacy of verification processes.

Ideally the system should be feasible and allow for flexibility of operations, so as to reduce the burden for economic operators.

The manufacturer or importer should not be permitted to mark any unit packet of tobacco product unless a previously approved anti-tampering solution is installed in the production line and is fully operational.

5.1.5.2. Competitive landscape

Anti-tampering technology has evolved through the development of a wide variety of products and solutions focused on addressing the different needs of the industry.

The review of solutions to potentially form part of the anti-tampering system aims to verify the legitimacy of the scanning activities in the verification process while maintaining the feasibility and flexibility of operation.

Image production controlling

This anti-tampering solution performs a visual control of the production process by capturing images of all the unit packages deployed in the production line that run through the scanning activities in the verification system. The solution achieves its purpose while doubling the functionalities: firstly by recording and taking pictures of the overall process, and secondly by adding the production counting feature.

Image production controlling transmits the recordings to the local storage, where they are stored for a limited time, allowing further inspection in case of tampering suspicions or audits. Furthermore, this equipment enables counting of the production, which allows identification of potential unauthorised tampering by comparing the number of unique identifiers transmitted through the verification system with the number of unit packets produced.

This type of equipment is used for traceability purposes in other industries, such as pharmaceutics and consumer packaged goods. It is also able to decode data carriers and transmit unique identifiers. A complete solution may integrate both a verification and anti-tampering systems in the same equipment, considerably reducing the burden for economic operators, while maintaining the flexibility of operations.

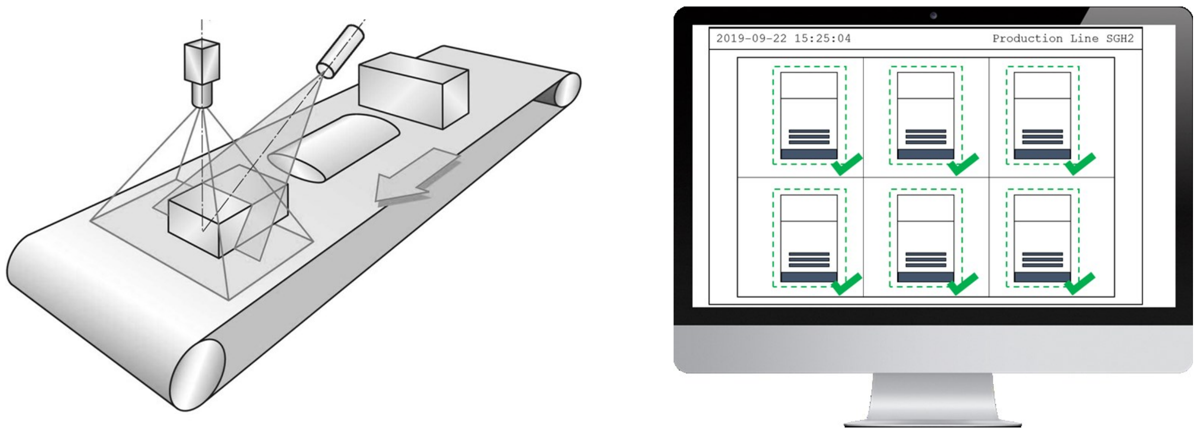


Figure 32: Image production controlling

CCTV video surveillance

The CCTV video surveillance solution deploys a number of cameras to control the verification system. The system records the adjacent areas near the scanning activities with the objective of registering any potential tampering attempt.

The system stores the recording locally for a limited time, allowing further inspection in case of tampering suspicions or audits. This enables identification of unauthorised tampering and does not affect manufacturer operations. Furthermore, video recognition applications could digitally detect potential unauthorised tampering attempts.

This technology is well-developed and widely used for security purposes, which reduces the associated burden. However, it does not control the manufacturing process by counting the production flow, unlike image production controlling. Therefore, this system will be useful when there is suspicion of tampering, but does not automatically provide alerts.

Figure 33: CCTV video surveillance

Counting manufacturing flow

This system counts the manufacturing flow entering the scanning activities in the verification system, which allows the identification of deviations between the number of unit packets produced and the count of unique identifiers verified. The result of this comparison can alert the competent authorities for further inspection.

This system is installed in the production line prior to the scanning activities in the verification system, and it sends the output to the local storage. It does not restrict the operational flow, guaranteeing the feasibility and flexibility of the process. However, this solution is only useful in automated production lines where operators do not directly influence the process, and is not useful in manual production processes.

Nevertheless, this solution may be used in combination with the CCTV video surveillance system. This combination both provides alerts and verifies the potential tampering activities by reviewing the CCTV video surveillance system recordings.

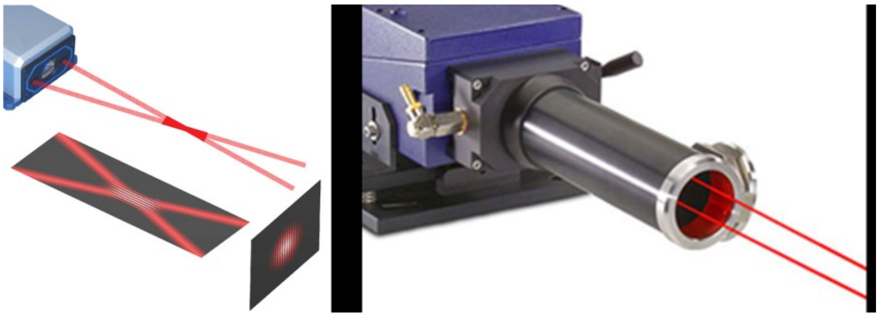


Figure 34: Manufacturing flow counter

5.1.5.3. Analysis of the solution elements

The anti-tampering solution protects the process of verifying unique identifiers following their applications, whilst maintaining the flexibility of operation and maximising the potential of reducing illicit trade.

In order to assess the most suitable solution for later implementation in the production lines, an analysis of the solution elements has been conducted. The proposed solutions were evaluated according three selection parameters:

- **Potential to reduce unauthorised tampering**. The ability of the device to assist authorities in identifying all potential or suspected cases of unauthorised interference/tampering.
- **Flexibility of operation**. The capacity of the device to comply with its mission while maintaining the correct functioning of operational processes.
- **Ability to count the production flow.** As an additional verification measure that alerts the system of interference in the process by comparing the count of the production flow with the number of unique identifiers registered by the scanning activities in the verification system.

Image production controlling

Image production controlling		
Potential to reduce unauthorised tampering	●	*The potential to reduce unauthorised tampering is high because the system records every unit packet entering the verification system. These images / records are stored locally, enabling further inspection.*
Flexibility of operation	●	*This solution is installed in the production line and is highly automated. It does not interrupt the material flow or restrict the production speed.*
Ability to count the production flow	●	*Solution's software is able to identify the number of unit packets entering the verification system, enabling the comparison with the number of verified unique identifiers.*

Table 29: Analysis of image production controlling system

CCTV video surveillance

CCTV video surveillance		
Potential to reduce unauthorised tampering	●	*The system records any movement surrounding the verification system, alerting of potential unauthorised tampering. These images / records are stored locally, enabling further inspection.*
Flexibility of operation	●	*This solution is not installed in the production line and it requires low maintenance. It does not interrupt the material flow or restrict the production speed.*
Ability to count the production flow	◔	*This system is not able to keep record of the production flow, therefore the additional verification measure resulting from the comparison of production count with verified unique identifiers cannot be deployed.*

Table 30: Analysis of CCTV video surveillance system

Counting manufacturing flow

Counting manufacturing flow		
Potential to reduce unauthorised tampering		*The system is able to control the production for later comparison; however, it cannot detect unauthorised tampering.*
Flexibility of operation		*This solution is installed in the production line and does not interrupt the material flow or restrict the production speed, although it may require additional operations (maintenance, reset…).*
Ability to count the production flow		*Solution's software is able to identify the number of unit packets entering the verification system, which adds security to the system by comparing with the number of verified unique identifiers.*

Table 31: Analysis of counting manufacturing flow system

5.1.5.4. Description of the anti-tampering solution

The anti-tampering solution should be able to assist in identifying potential or suspected cases of unauthorised interference/tampering. As previously stated, the manufacturer or importer shall not be permitted to mark any unit packet of tobacco products unless the anti-tampering solution has previously been installed and is fully operational.

Since there is a wide variety of manufacturing lines, and based on the analyses made in previous sections, this report proposes three options for anti-tampering solutions to best meet manufacturer needs. These are categorised according to the automation level of the manufacturing lines.

Automated manufacturing lines

Option 1.1 – Image production controlling

This option proposes the use of image production controlling as the anti-tampering solution in the manufacturing lines of tobacco products. As the highest ranked solution according to the three selection criteria (potential to reduce tampering, flexibility of operation and ability to count the production flow), image production controlling is the most suitable option to accomplish the requirements of the TPD in terms of anti-tampering.

This solution prevents tampering with the marking of unit packets by comparing the unit packet production with the number of unique identifiers reported to the Primary Data Storage. Additional applications can be built from the data recorded, establishing real-time alerts or providing valuable insight for further audits or inspections. Moreover, this anti-tampering solution should be equipped with uninterrupted power supply (UPS) device so that it keeps working in case of disconnection from its primary power source.

This type of solution has already been tested in the tobacco industry (Art 27 Brazilian Law 12402, s.f.), and it is especially appropriate for high-speed production lines where production speed is a critical element of the process. Additionally, the equipment may perform both verification and anti-tampering prevention activities, significantly reducing the burden for manufacturers.

Although the images are stored locally, the external third party has access to them for periodical audits or for inspection in case of suspicion of fraud.

Option 1.2 – CCTV video surveillance with production control

The second option is a system based on two solutions: CCTV video surveillance and production control through counting manufacturing flow. This solution does not present a severe burden and it is envisioned for manufacturers with automated production lines.

It combines the security component of the CCTV video surveillance with the ability to detect potential unauthorised tampering attempts when comparing the production count with the number of unique identifiers sent to the Primary Data Storage. Moreover, this anti-tampering solution should be equipped with uninterrupted power supply (UPS) device so that it keeps working in case of disconnection from its primary power source.

The recordings are stored locally and the external third party has access to them for periodical audits or for inspection in case of suspicion of fraud, especially when the solution detects a variation between the number of unique identifiers reported and production count.

Non-automated manufacturing lines

Option 2.1 – CCTV video surveillance in non-automated manufacturing lines

This option proposes a system based on CCTV video surveillance that keeps record of the activities near the verification system. This solution is especially envisioned for manufacturing facilities with a low production rate, where production is not fully automated and uses a variety of manual processes.

This type of solution has been widely used in a multitude of industries, being proven as an effective answer to security issues. Additionally, it does not represent a significant burden for manufactures, does not affect the operational flow, and is an attractive option for small and medium manufacturers. Moreover, this anti-tampering solution should be equipped with uninterrupted power supply (UPS) device so that it keeps working in case of disconnection from its primary power source.

The recordings are stored locally and the external third party has access to them for periodical audits or for inspection in case of suspicion of fraud.

5.2. IT artefacts

The IT domain encompasses all the capabilities related to the information flows in the Tracking and Tracing System. This subchapter on the technical specifications for the IT artefacts aims to provide a clear view regarding the following:

- Temporary Buffer (optional): describes the function of the optional component that reports events from the facilities to the Tracking and Tracing System.

- Primary Data Storage: describes the function of the Primary Data Storage, a storage solution that hosts data exclusively related to a specific manufacturer or importer.
- Surveillance Data Storage: the storage solution that hosts a global copy of the distributed data.
- ID Issuer: describes the function of the ID Issuer, an agent in charge of providing the economic operators with unique identifiers.
- Overall data flow: the diagram that depicts the flow of information between the main agents involved in the Tracking and Tracing System.
- Messages: describes the structure of the messages exchanged throughout the system.
- Data dictionary: includes a catalogue of the main entities that shall be stored by the Primary and Surveillance Data Storages.

In addition, Chapter 3 of Annex II*: "Detailed technical specifications for the IT artefacts of the Tracking and Tracing System"* further develops the topics contained in the table below:

Subsection	Content
3.1	System architecture
3.2	Sequence diagrams
3.3	Data flow diagram
3.4	Temporary Buffer (optional)
3.5	Message
3.6	System users
3.7	Primary Data Storage
3.8	Surveillance Data Storage
3.9	Repository Router
3.10	Data dictionary
3.11	Common validation rules for the data
3.12	Security policy
3.13	Confidentiality policy
3.14	Contingency plan

Table 32: Annex II – Chapter 3: Detailed technical specifications for the IT artefacts of the Tracking and Tracing System

5.2.1. Temporary Buffer (optional component)

The Temporary Buffer is an **optional** component, established on a voluntary basis by the economic operators at a facility level, which **reports events** required to the Tracking and Tracing System. It is recommended as it allows to **decouple** the manufacturing and distribution activities from the transmission of events and also **mediates communication** between data sources of the economic operators' proprietary solutions and the Tracking and Tracing System.

The Temporary Buffer should collect data events from a number of devices from the economic operators (e.g. production lines, scanners, etc.). Moreover, the Temporary Buffer should act as a central gateway at a facility level and should be responsible for aggregating these data events and transmitting them to the Tracking and Tracing System. The transmission of events is not required to be done in real time nor is it required that the production/logistic processes wait for a delivery acknowledgement.

To this aim, the Temporary Buffer should use a **local storage as an upstream queuing system** for outgoing messages. This local storage would act as a safety buffer to temporarily hold data events as they are received in the Temporary Buffer component, serving as a short-term assurance against any service interruption in the upper layer (i.e. Primary Data Storage and Surveillance Data Storage), which is receiving the data stream.

Finally, it should be noted that the Temporary Buffer **does not manage the integration with the economic operator's legacy systems**, because it is assumed that all the necessary information (e.g. trade data) has been collected previously.

5.2.2. Primary Data Storage

The **Primary Data Storage** is a performance-critical solution that shall be able to operate at large-scale. The quality properties that will measure the performance of the system are: security, resilience or fault tolerance, low-latency response, high availability, on-demand scalability, and efficiency. The main capabilities to be supported are: management of large volumes of data, load data continuously, data integrity, system availability, administration and configuration. Section 3.7.1 of "*Annex II provides the detailed list of technical specifications*".

The input data flow of the Primary Data Storage comprises a variety of events which are collected at a high frequency from different sources through the following data flows:

- Reported directly by the manufacturer or importer at facility level;
- Routed through the Repository Router of the Surveillance Data Storage solution, which receives the messages from the distributors/wholesalers.

Therefore, the Primary Data Storage must be able to handle data at high performance levels and on a large-scale, in order to support current and future workloads. The Primary Data Storage is responsible for persisting the messages, consolidating traceability information, delivering a copy of them to the Surveillance Data Storage, and conducting data analytics while also supporting high rates of message throughput for input/output operations.

The Data Acquisition and Data Processing components of the Primary Data Storage should be designed based on an **event-driven architectural pattern** to manage the massive number of events expected and of system transactions. This will require technologies that support event-driven design, such as message queuing, publish-and-subscribe systems and stream-processing middleware. The event-driven architectural pattern will allow routing events to the relevant event handlers, scaling the capacity of the system up and down, and contextualising the information captured. This event-centric approach has additional features, such as improved performance and resilience (Mark Richards, 2015). For example, event streams can be shared and distributed on several servers to increase throughput and reduce latency. There are also architectural patterns like event sourcing (Betts, Dominguez, Melnik, Simonazzi, & Subramanian, 2013) that help preserve integrity in the eventual consistency scenarios by storing event logs (rather than computed states), which can be retrofitted to enable fault tolerance. Thus, request- and event-driven interactions with the economic operators can be managed seamlessly.

The recommended event-driven topology to be applied is the **broker topology**, where the message flow is distributed across the *event processor* components in a chain-like fashion through a message broker engine. This topology requires two components: a broker component and an *event processor* component. The broker component can be centralised or federated and contains all of the event channels used within the event flow. The event channels contained within the broker component can be message queues, message topics, or a combination of both. The *event processor* components listen to the event channels, receive the event from the event broker, and execute specific business logic to process the event. The *event processor* component is an individual and independent module with very specific responsibilities. Hence, each *event processor* component processes an event accordingly and publishes a new event, triggering the next action to be performed.

Thus, the **Data Acquisition** component must include (but not be limited to) the following *event processor* components:

- Authentication. It resolves and authenticates the sender’s identity against a trusted identity provider. If the message is sent from an unauthenticated sender, it shall not be accepted.
- Compliance. It verifies the event compliance with the expected schema of the message. If it is not compliant, it shall not be accepted.
- Duplication. It verifies that this same event has not been received before. The system shall not accept a duplicated event, because tracking and tracing messages are not intrinsically idempotent (e.g. if the same aggregation message is processed more than once, it may cause an integrity issue).
- Storage. It stores the event as is, without any processing. If it is not stored correctly, the system shall return a proper error. As a general rule, it segregates access to data belonging to different companies in order to keep the commercially sensitive information of each manufacturer or importer separate.
- Acknowledgment. It returns a positive acknowledgement of the message reception if the previous steps are successfully accomplished (i.e. non-repudiation). If some of the previous steps have failed, it should return a negative acknowledgement.

Once acquired, the events are ingested by the Data Processing component pipeline for refining and ensuring data integrity prior to their consolidation in the storage. Thus, the **Data Processing** component must include (but not be limited to) the following *event processor* components:

- Data cleaning. It cleans data by filling in missing values, smoothing noisy data and resolving inconsistencies.

- Data copy. It sends a copy of the message to the Surveillance Data Storage.
- Data integrity. It shall be assured by guaranteeing the completeness, consistency, accuracy and reliability of data. Thus, at least the following integrity constraints shall be enforced:
    - Default integrity constraints: primary keys, entity integrity, foreign keys and referential integrity.
    - Specific integrity constraints, which are domain specific and are also referred to as common validation rules (these constraints are detailed in section 3.11 of "*Annex II: Technical Specifications of the Tracking and Tracing System*".
- Data consolidation. The relevant information included within the message shall be consolidated into the underlying storage, when appropriate and possible (i.e. it is not an orphan event). Furthermore, the consolidation process shall manage the message recall capability. This capability allows economic operators to send a recall request for any event previously reported, if an error is later detected. The recall implies that the storage flags the event as cancelled and notifies if the recall concerns a message that is not the last element in the history of operational/transactional events for a given unique identifier.

It should be noted that the economic operators are not constrained to submit events in the temporal order they occurred, so the events may arrive in any order to the Primary Data Storage. When an event is transmitted prior to the transmission of other related events that in fact, occurred at an earlier point in time, this event can be considered an orphan event. Therefore, the Data Processing component should implement an eventual consistency model, keeping orphan events in a queue. Once all the previous events of the sequence of an orphan event arrives to the system, the Data Processing component must consume the orphan event from the queue. Due to this asynchronous processing and the maximum allowed delay of near real-time for transmitting events, data exploitation capabilities such as reporting or analytics cannot be done in real time. Thus, a minimum delay of one hour should be considered for data timeliness when exploiting data (e.g. reporting or analytics).

While moving the events through the Data Processing pipeline stages, their state will follow the flow depicted below:

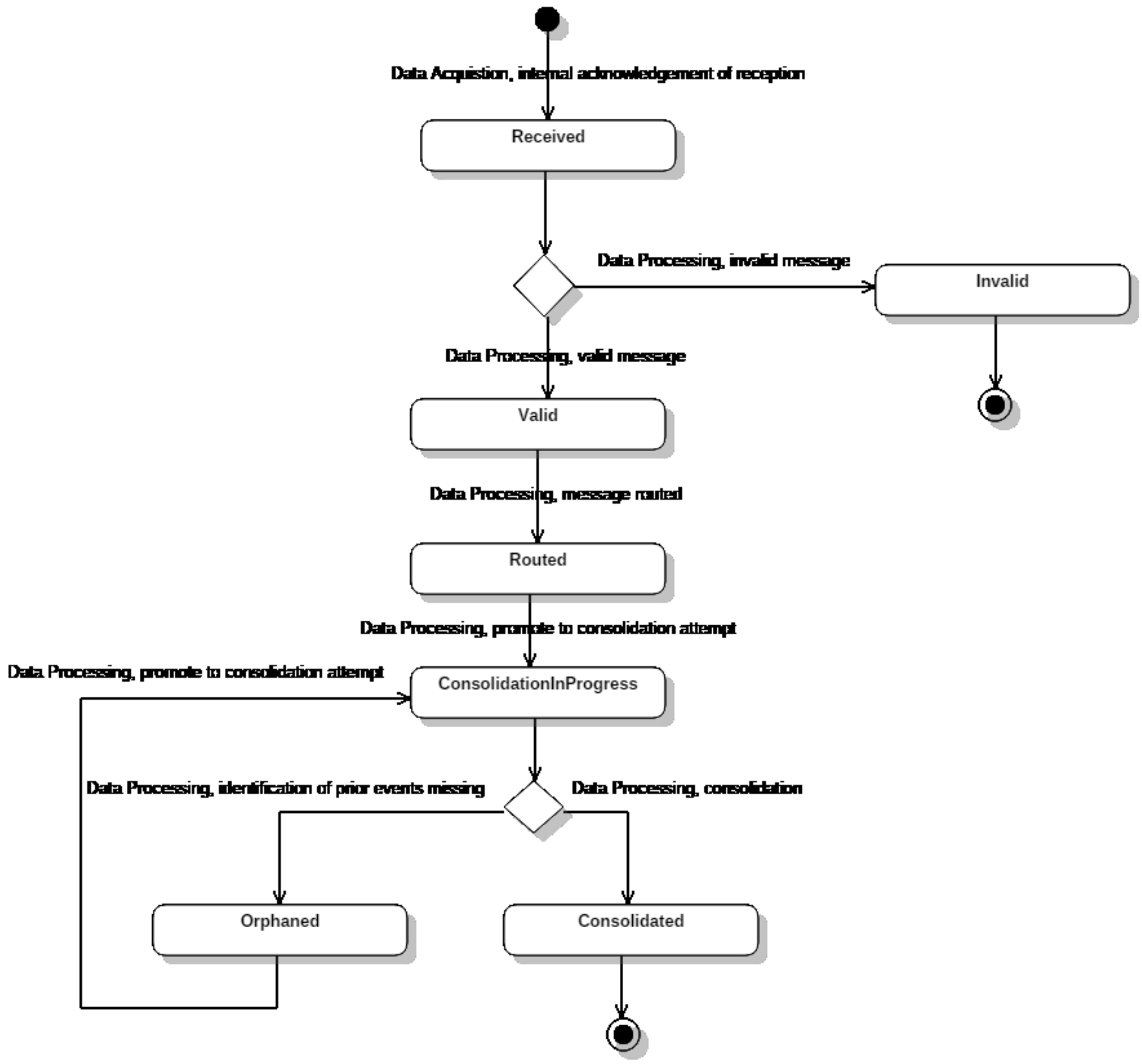


Figure 35: Event state diagram

In order to decouple read accesses from write accesses, the **Data Consumption** component will be responsible for:

- Hosting capabilities to exploit data such as reporting, dashboards, data analytics, query tools, bulk data extraction, and alert tools. These engines will access the data that has been successfully consolidated and will provide end users (i.e. competent authorities, the Commission, auditors and key users) with the data that they are requesting or are subscribed to.
- Publishing standard and secure interfaces that enable the secure exchange of relevant data with external systems (i.e. competent authorities and auditors), which have been previously authorised, using the canonical data model (see section 3.10.3 of "*Annex II: Technical Specifications of the Tracking and Tracing System*").

The Primary Data Storage also includes a set of **cross-cutting services** that will support the functioning of the other components; namely: security, administration, configuration, and monitoring.

Concerning the storage accesses and privileges, it is important to note that: a) economic operators are only allowed to transmit reports; b) the Commission, competent authorities and independent external auditors are the only users who have access to the stored data; c) only in duly justified cases (e.g. during an investigation), the Commission or the Member States may provide data to manufacturers or importers; and d) manufacturers and importers shall conclude contracts, which are to be approved by the Commission, with the third party data storage provider, but do not have any control over the storage.

Finally, the following additional considerations should be applied, with regard to scalability and availability, in the detailed Primary Data Storage design provided by the provider:

- The Primary Data Storage must be able to scale horizontally to add more storage or processing capacities, if necessary. A candidate strategy for scaling out the storage would be sharding (Michael T. Fisher; Martin L. Abbott, 2015).
- Redundant data storage is required to ensure high-availability. Data from an active instance must be backed up on at least a secondary storage. Regardless of the redundancy level used (one or several instances could be active at a time), the infrastructure must mirror the data to the other instances in near real-time.
- Tiered storage is also required to attain better performance for the data analytics and data consumption capabilities while reducing the overall storage cost.
- Data archiving is required to move data that is not actively used to an offline data storage. This archived data can be imported back into its respective data storage, if necessary. The data archiving must be configured with predefined rules, and carried out only by authorised users.
- The third party provider will develop, operate and maintain high-performance, standard and economy implications of managing data in the data storages, as well as relevant procedures to safely move data between tiers and between storages.
- The Primary Data Storage solution should be designed to be highly fault-tolerant and continue operation, even at a reduced level, despite any failure. The solution should be able to detect errors caused by faults, assess the damage caused by the fault, recover from the error, and isolate the fault.
- Each of the main components of the Primary Data Storage solution shall be designed to be fault-isolative, in order to not propagate its errors to other components of the solution and limit the impact of any problem to the component itself. With this fault isolation approach, the overall solution is protected and allows for graceful failure under extremely high demand, thereby not bringing the entire solution down. Additional benefits include increased availability, scalability and resilience. A candidate pattern for the fault isolation implementation is the circuit breaker (Michael T. Fisher; Martin L. Abbott, 2015).

5.2.3. Surveillance Data Storage

Although the **Surveillance Data Storage** shares many qualities and capabilities with the Primary Data Storage, this section fully describes the Surveillance Data Storage. As such, misinterpretations are avoided and comprehensive explanations of the target system are provided. Therefore, the descriptions below will be very similar to that of the Primary

Data Storage above, but applied to the Surveillance Data Storage with the following main differences:

- The Surveillance Data Storage includes a Repository Router component that receives: a) all the messages transmitted from the distributors and wholesalers; and b) all the messages from ID Issuer solutions about generated serial numbers. This component is responsible for routing these messages to the Primary Data Storages that shall consolidate the data that corresponds to them (i.e. the information of tobacco products that are manufactured or imported by the manufacturer/importer that has established the Primary Data Storage).
- The Surveillance Data Storage receives a copy of all the messages that have been managed by the decentralised Primary Data Storage solutions.

The Surveillance Data Storage is also a performance-critical system and the same quality measures and main capabilities as the Primary Data Storage apply. The Surveillance Data Storage must also support analytics and reporting requirements, addressing a group of users that only consume processed data. Section 3.8.1 of Annex II provides the detailed list of technical specifications.

The input data flow of the Surveillance Data Storage comprises a variety of events which are collected at a high frequency from the following sources:

- ID Issuer solution(s);
- Facilities from distributors/wholesalers;
- The distributed Primary Data Storages.

To this end, the Surveillance Data Storage must be able to handle data at high-performance levels and on a large-scale, in order to support current and future workloads. The Surveillance Data Storage is responsible for persisting the messages, consolidating traceability information, routing them to the Primary Data Storage if necessary, and conducting data analytics, while also supporting high rates of message throughput for input/output operations.

The Data Acquisition, Data Processing and Repository Router components of the Surveillance Data Storage should be designed based on an **event-driven** architectural pattern to manage the massive number of events expected and the system transactions. This will require technologies that support event-driven design, such as message queuing, publish-and-subscribe systems, and stream-processing middleware. The event-driven architectural pattern will allow routing of events to the relevant event handlers, scaling the capacity of the system up and down, and contextualising the information captured. This event-centric approach has additional features, such as improved performance and resilience (Mark Richards, 2015). For example, event streams can be shared and distributed on several servers to increase throughput and reduce latency. There are also architectural patterns like event-sourcing (Betts, Dominguez, Melnik, Simonazzi, & Subramanian, 2013) that help preserve integrity in the eventual consistency scenarios by storing event logs (rather than computed states), which can be retrofitted to enable fault tolerance. Thus, request- and event-driven interactions with the economic operators can be managed seamlessly.

The recommended event-driven topology to be applied is the **broker topology**, where the message flow is distributed across the event processor components in a chain-like fashion through a message broker engine. This topology requires two components: a *broker* component and an *event processor* component. The broker component can be centralised or federated and contains all of the event channels that are used within the event flow. The event channels contained within the broker component can be message queues, message topics, or a combination of both. The event processor components listen to the event channels, receive the event from the event broker, and execute specific business logic to process the event. The event processor component is an individual and independent module with very specific responsibilities. Hence, each event processor component accordingly processes an event and publishes a new event that triggers the next action to be performed.

Repository Router

The Repository Router will handle significant volume of data events because the ID Issuer solutions and the reporting components of distributors and wholesalers will push a massive influx of data events to be routed. Therefore, the Repository Router must include (but not be limited to) the following *event processor* components:

- Acquisition. It will rely on the Data Acquisition component.
- Routing. It is responsible for sending to the Primary Data Storages of the different manufacturers/importers the events that are relevant for them. The event data can take multiple paths depending on the manufacturer/importer of the items referred to in the event.

Data Acquisition

As with the Primary Data Storage, the **Data Acquisition** component will manage the overall data ingestion. Thus, the Data Acquisition component must include (but not be limited to) the following *event processor* components:

- Authentication. It resolves and authenticates the sender's identity against a trusted identity provider. If the message is sent from an unauthenticated sender, it shall not be accepted.
- Compliance. It verifies the event compliance with the expected schema of the message. If it is not compliant, it shall not be accepted.
- Duplication. It verifies that this same event has not been received before. The system shall not accept a duplicated event, because tracking and tracing messages are not intrinsically idempotent (e.g. if the same aggregation message is processed more than once, it may cause an integrity issue).
- Storage. It stores the event as is, without any processing. If it is not stored correctly, the system shall return an error notification. As a general rule, it segregates access to data belonging to different companies, in order to preserve the commercially sensitive information of each manufacturer or importer separate.
- Acknowledgment. It returns a positive acknowledgement of the message reception if the previous steps are successfully accomplished (i.e. non-repudiation). If some of the previous steps have failed, it returns a negative acknowledgement.

It should be noted that the economic operators are not constrained to submit events in the temporal order they occurred, so the events may arrive in any order. When an event is transmitted prior to the transmission of other related events that occurred at an earlier time, this event can be considered an orphan event. Therefore, the Data Processing shall implement an eventual consistency model, keeping orphan events in a queue. Once all the previous events of the sequence of an orphan event arrives to the system, the Data Processing component must consume the orphan event from the queue. Due to this asynchronous processing and the maximum allowed delay of one hour for transmitting events, data exploitation capabilities such as reporting or analytics cannot be done in real time. Thus, a minimum delay of one hour should be considered for data timeliness when exploiting data (e.g. reporting or analytics).

Since the Repository Router plays a major role in deploying the scalable Tracking and Tracing System, the communication between the reporting components of economic operators (e.g. Temporary Buffer) and the Repository Router should use a TCP-based data streaming protocol. The reporting component, which pushes the data to the Repository Router, may initiate a socket connection and then uses it to write requests and read back the corresponding responses. The communication between the Repository Router and the Primary Data Storage should work in a similar way. Additionally, the Repository Router shall be able to connect to multiple instances of the Primary Data Storages to submit data.

The use of a brokered protocol based on raw TCP sockets may offer better performance and throughput at scale than using request/response protocol for ingestion. This observation is best supported by the fact that the use of data transfer protocols like HTTP, which require a handshake for each connection/disconnection, adds unneeded overhead to the transmission of small chunks of data.

Once accepted by the Data Acquisition component, the events are ingested by the Data Processing component pipeline for refining and ensuring data integrity prior to their consolidation in the storage. Thus, the Data Processing component must include (but not be limited to) the following *event processor* components:

- Data cleaning. It cleans data by filling in missing values, smoothing noisy data, and resolving inconsistencies.
- Data copy. It sends a copy of the raw message to the Surveillance Data Storage.
- Data integrity. It shall be assured by guaranteeing the completeness, consistency, accuracy and reliability of data. Thus, at least the following integrity constraints shall be enforced:
    - Default integrity constraints: primary keys, entity integrity, foreign keys, and referential integrity.
    - Specific integrity constraints, which are domain specific and are also referred to as common validation rules (these constraints are detailed in Annex II).
- Data consolidation. The relevant information included within the message shall be consolidated into the underlying storage, when appropriate and possible (i.e. it is not an orphan event). Furthermore, the consolidation process shall manage the message recall capability. This capability allows that the economic operators to send a recall request for any event previously reported, if an error has later been detected. The recall implies that the storage flags the event as cancelled and

notifies if the recall concerns a message that is not the last element in the history of operational/transactional events for a given unique identifier.

While moving the events through the Data Processing pipeline stages, their state will follow the same flow depicted above.

In order to decouple read accesses from write accesses, the **Data Consumption** component will be responsible for:

- Hosting capabilities to exploit data such as reporting, dashboards, data analytics, query tools, bulk data extraction, and alert tools. These engines will access the data that has been successfully consolidated and will provide end users (i.e. competent authorities, the European Commission, auditors and key users) with the data that they are requesting or are subscribed to.
- Publishing standard and secure interfaces that enable the secure exchange of relevant data with external systems (i.e. competent authorities and auditors), which have been previously authorised, using the canonical data model (see section 3.10.3 of Annex II for more details).

The Surveillance Data Storage also includes a set of **cross-cutting services** that will support the functioning of the rest of the components, namely: security, administration, configuration, and monitoring.

Concerning the storage accesses and privileges, it is important to note that: a) economic operators are only allowed to transmit reports; b) the Commission, competent authorities and independent external auditors are the only users who have full access to the stored data; and c) only in duly justified cases (e.g. during an investigation), the Commission or the Member States may provide data to manufacturers or importers.

Finally, the following additional considerations should be applied, with regard to the scalability and availability, in the detailed Surveillance Data Storage design provided by the provider:

- The Surveillance Data Storage must be able to scale horizontally to add more storage or processing capacities, if necessary. A candidate strategy for scaling out the storage would be sharding (Michael T. Fisher; Martin L. Abbott, 2015).
- Redundant data storage is required to ensure high-availability. Data from an active instance must be backed up on, at least, a secondary storage. Regardless of the redundancy level used (one or several instances could be active at a time), the infrastructure must mirror the data to the other instances in near real-time.
- Tiered storage is also required to attain better performance for the data analytics and data consumption capabilities while reducing the overall storage cost.
- Data archiving is required to move data that is not actively used to an offline data storage. This archived data can be imported back into its respective data storage, if necessary. The data archiving must be configured with predefined rules, and carried out only by authorised users.
- The third party provider will develop, operate and maintain high-performance, standard and economy implications of managing data in the data storages, as well as relevant procedures to safely move data between tiers and between storages.
- The Surveillance Data Storage solution should be designed to be highly fault-tolerant and continue operation, even at a reduced level, despite any failure. The

solution should be able to detect errors caused by faults, assess the damage caused by the fault, recover from the error, and isolate the fault.

- Each of the main components of the Surveillance Data Storage solution shall be designed to be fault-isolative, in order to not propagate its errors to other components of the solution and limit the impact of any problem to the component itself. With this fault isolation approach, the overall solution is protected and allows for graceful failure under extremely high demand, thus not bringing the entire solution down. Additional benefits are increased availability, scalability and resilience. A candidate pattern for the fault isolation implementation is the circuit breaker (Michael T. Fisher; Martin L. Abbott, 2015).

5.2.4. ID Issuer

The **ID Issuer** is also a part of performance-critical system that shall be able to operate on a large-scale. The quality properties that will measure the performance of the ID Issuer solution are as follows: security, resilience or fault tolerance, low-latency response, high availability, on-demand scalability, and efficiency. The main capabilities that shall be supported are: dynamic generation of large volumes of serial numbers, manage large volumes of serial numbers, delivery of serial numbers, data integrity, system availability, administration and configuration. Annex II provides the detailed list of requirements.

The Tracking and Tracing System comprises one ID Issuer solution per Member State, who appoints the independent third party serial number provider that will establish the solution.

The output data flow of the ID Issuer comprises an efficient assurance of delivery of serial numbers to the following recipients:

- Surveillance Data Storage. It should be noted that the Surveillance Data Storage routes this information later to the Primary Data Storage;
- Economic operators that have requested sets of serial numbers.

To this end, the ID Issuer solution must be able to handle parallel computations at high-performance levels and at large-scale, in order to support current and future workloads. The ID Issuer solution is responsible for generating serial numbers, verifying their uniqueness and randomness, notifying the Surveillance Data Storage of the serial numbers, and also supporting concurrent computing for the generation and verification of high volumes of serial numbers.

The responsibilities of the ID Issuer solution are threefold:

a) Offer services to the economic operators in order to provision serial numbers for their activities;

b) Notify the central Surveillance Data Storage solution of which serial numbers have been provisioned. This notification also includes the Primary Information block with the reference data that was provided by the economic operator. The notification shall be done prior to delivering the serial numbers to the economic operators.

c) Offer registration services to the economic operators. These registration services allow the population of lookup data needed for unique identifier serialisation. The lookup registers are related to: economic operator, facility of manufacturing, and machine of manufacturing.

Two types of serial numbers can be generated:

- Serial numbers for unit packets of tobacco products. This generation shall follow the rules laid down in Section 5.1.1.2. It is expected that these serial numbers will be requested only by manufacturers or importers.
- Serial numbers for aggregation packaging levels. This generation shall follow the rules laid down in Section 5.1.2.2. It is expected that these serial numbers will be requested by any economic operator.

5.2.5. Overall data flow

The diagram below shows the overall data flow discussed previously. The symbol notation meaning is as follows:

- Grey (): actors
- Green (): component that stores data
- Blue (): processes that activate the data flow
- The arrow points to the target storage where the data is saved.

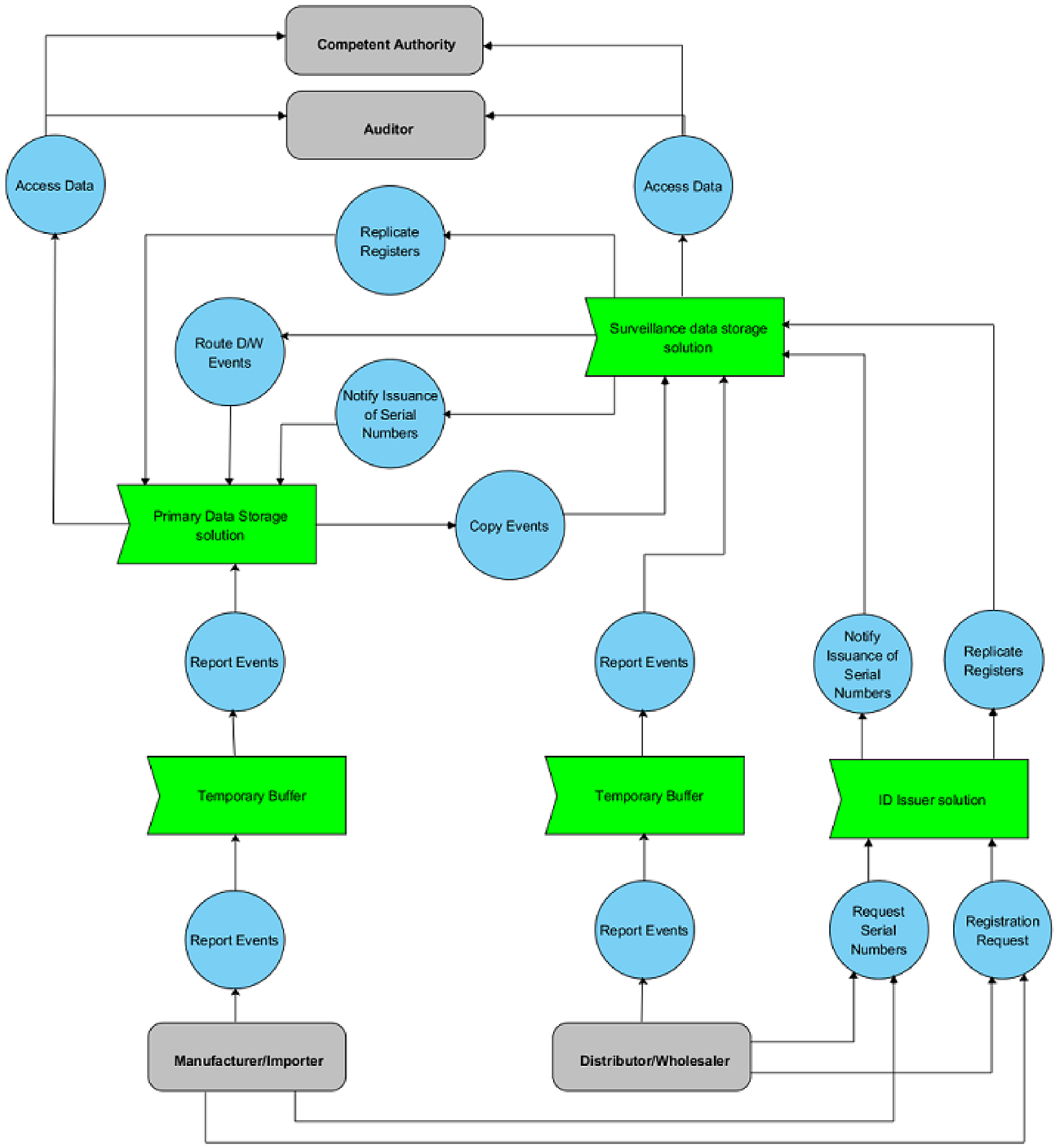


Figure 36: Tracking and Tracking main data flows

These data flows are derived from the business process diagrams (see Section 1.3 of Annex II).

5.2.6. Messages

The following section describes the specification of the structure of the messages exchanged through the Tracking and Tracing System.

The message exchange provides resources for two parties to conduct electronic business by the exchange of business documents. The sending party packages one or more documents into a request message, which is then sent to the receiving party. The receiving party processes the message contents and responds to the sending party. Examples of the sending party's documents may be a request for the issuance of serial numbers and the reporting of events information. Examples of the receiving party's responses may include processed data or simple acknowledgements (W3C – World Wide Web Consortium, 2017).

The data exchange scenario of this system requires a request/response message feature. A request containing a business document is sent by a sender to a receiver when a business application is invoked. The business application processes the request and generates a response, which is returned to the sender that originated the request. The sender is informed by the receiver of the status (successful or otherwise) of the request message delivery, with the obligation to communicate whether the message was successfully delivered and accepted or if a failure occurred that prevented the successful delivery.

Long-running process

If the sender sends a message that invokes a long-running business process, the same basic request/response pattern occurs as previously described. The difference is that the request and response messages are separated in time and implemented as distinct unidirectional messages, and the sending application does not block and wait for the final processing response to return. In this situation, the receiver responds to the requestor with an acknowledgment message containing a request identifier, which will later be used by the requestor to check on the status of the process or to retrieve the final results.

Acknowledgement

The acknowledgement is a message exchange agreement mechanism to notify the sender about the success or failure of the message sending to the receiver. It is a simple return message communicating the success or the failure of the data exchange transaction.

Retry policy

The acknowledgement ensures the successful delivery of a message by the receiver. When it is not possible to achieve such confirmation, the retry policy must exist in order to define the next attempts to deliver the message. The retry policy parameters specify the number of times the sender should resend an unacknowledged message before giving up and deciding the message cannot be delivered, and taking an alternative action. The sender must not resend messages more than the allowed number of times specified in the retry policy.

No comment is made by this document on retry behaviour, as it shall be decided during the implementation and is highly dependent on the technology. For instance, if a SOAP message is sent over FTP and the TCP/IP connection cannot be made due to a network problem it would seem reasonable for the transport to automatically retry. This retry is not considered when counting acknowledgement retries.

Retry interval

The retry interval specifies the time a sender must wait between retries. The sender is expected to wait the full retry interval after sending a request before retrying the request send, and then to wait the retry interval between all subsequent retries. If an acknowledgement is received, the sender must not repeat the request. For the cases that an acknowledgement is not received after various retries, the retry policy must define a limit on the number of send attempts before the sender takes an alternative action in order to handle the undeliverable message problem. This action may be the simple discard of the undelivered message or include several steps, such as keeping the message in a queue for future attempts and informing the team responsible for deciding how to solve the problem.

The messaging does not specify how the data should be acquired nor computed from the distinct type of sources. It isolates the message exchange from the abstracted level of the data capture architecture.

Error handling

The message exchange mechanism provides the means for handling errors. Faults that occur during the message exchange are referred to as exceptions. When an activity fails, it throws an exception, returning a message corresponding to one of the errors listed in the system errors catalogue.

5.2.7. Data dictionary

The data dictionary described below includes a **catalogue of the main entities** that shall be stored by the Primary and Surveillance Data Storages. This catalogue also includes technical details such as data type, cardinality, priority and relationships with other entities.

In order to ensure interoperability and a consistent data exchange between all Data Storages, it is recommended that the data dictionary is established by the provider of the Surveillance Data Storage. The data dictionary provides a **bottom-line logical data definition,** which can be extended, if necessary, by the independent third party data storage provider that establishes the Primary or Surveillance Data Storage. It is up to the providers to decide on the final details of the physical storage, as long as they are compatible with the data dictionary. As such, flexibility and extensibility are promoted because new entities and additional information per entity could be accommodated on top of this common data dictionary. With this approach, the storage provider could save supplementary information needed to realise the functionalities required by the Tracking and Tracing System.

It should be noted that there are certain capabilities, such as **data analytics,** that have been intentionally excluded from the definition because of their complex nature and the lack of standard information models. Hence, competition is promoted because providers will be not constrained to work with a fixed definition. As such, they will be able to propose their best-of-breed approach based on their own expertise and supporting data structure.

In order to provide a compelling and accurate data dictionary, the following sources have been verified: (Cornelis Adrianus van Dorp, 2004), (L Ruiz-Garciaa; G. Steinbergerb; M. Rothmundc, 2010), (ISO/IEC 19988:2015 CBV, 2015), (ISO/IEC 19987:2015 EPCIS, 2016) and (DG SANTE - Tobacco products data dictionary for submission, 2016).

The following diagram depicts the main entities of the data dictionary and their relationships:

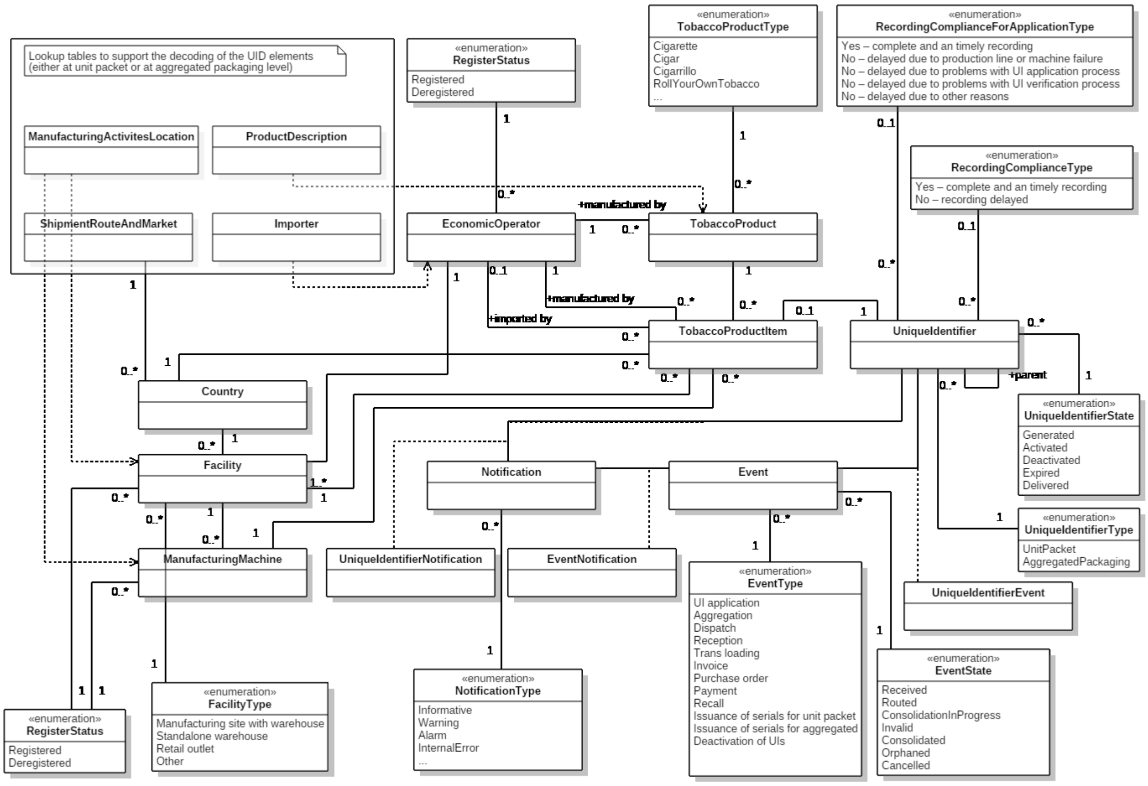


Figure 37: Data dictionary entities diagram

6. MODEL CONTRACT FOR THE THIRD PARTY DATA STORAGE

According to article 15(8) of the Tobacco Products Directive, Member States shall ensure that the manufacturers and importers of tobacco products conclude data storage contracts with an independent third party, for the purpose of hosting the data storage facility for all relevant data.

A proposal for such contract ("Agreement") can be found on Annex III of this report ("Model contract for the third party data storage"). The Agreement is to be signed between the manufacturers/importers and the providers of the data storage data services ("the Contractor", as of the terms of the Agreement).

The Agreement is structured as follows:

- **General Terms of Service**: Intended to regulate the provisions of the Data Storage services, which must be complemented with the requirements set out in Annexes 1, 2 and 3, and understood under the light of Annex 4.
- **Annex 1: Requirements Specification**: Includes the technical specifications of the service, and it is structured as follows:
    - Primary Data Storage
        - Requirements Specifications
            i. Functional
            ii. Technical
                a. System qualities
                b. Security
                c. Data Protection
                d. System constraints
                e. System interfaces
            iii. Applicable standards
    - Surveillance Data Storage
        - Requirements Specifications
            i. Functional
            ii. Technical
                a. System qualities
                b. Security
                c. Data Protection
                d. System constraints
                e. System interfaces
            iii. Applicable standards
    - Repository Router
        - Requirements Specifications

   i. Functional
   ii. Technical
      a. System qualities
      b. Security
      c. System constraints

- **Annex 2: Service Level Agreement**: Intended to regulate specific aspects of the service, in terms of quality, responsiveness and availability of the service to be provided by the Contractor.
- **Annex 3: Price Conditions:** As developed throughout the report, the Surveillance Data Storage shall be the central solution hosting a global copy of the distributed data generated by the system. It shall provide service to the manufacturers and importers, and also to the economic operators in the supply chain (wholesalers and distributors).

  In order to fairly split the cost of the Surveillance Data Storage amongst all the importers and manufacturers of tobacco products, a price scheme is proposed in the Price Conditions of the Agreement. The total monthly price of the service to be paid by the manufacturers and importers is the sum of:

  - A share of the total fix costs of the solution, calculated pro-rata based on the share of unique identifiers stored in the Surveillance Data Storage each month.
  - A variable price, with a unitary cost per unique identifier stored, based on the number unique identifiers stored by each manufacturer/importer
- **Annex 4: Definitions:** In the Agreement, all terms shall have the same meaning as defined in Article 2 of the Tobacco Products Directive, unless specifically provided in the Agreement. Such terms and their definitions are set out in Annex 4.

7. TECHNICAL SPECIFICATIONS FOR THE SECURITY FEATURES

This chapter aims to provide information on the following topics:

- Legal requirements: Identification of the primary requirement of the Implementing Act to be adopted by the European Commission related to the security features under Article 16 of the TPD.
- Technical requirements: Identification of types of security features, divided by categories and components compatibility.
- Operational requirements: Highlight security feature considerations in terms of needs (such as controls, security, cooperation between manufacturers and Member States, ease of enforcement / authentication, and size and placement rules).
- Rotation rules: Provide an overview of potential security feature rotation rules.

7.1. Legal requirements

Article 16 of the TPD requires tamper-proof and irremovable security features, composed of visible and invisible elements, on all unit packets of tobacco products placed on the market, as a method to fight illicit trade.

- **Tamper-proof (Tamper-evident).** Features, including techniques, which provide evidence of tampering attempts and elements to prevent transfer and reuse.

  Examples of methods to add tamper resistance to a security package include:

  - Slits: Cuts or partial cuts in the substrate so that it breaks apart if removal is attempted or the integrity of the material is compromised by cutting or piercing; material which breaks apart in this way is termed "frangible".
  - Voiding: Use of cuts, adhesives or inks which leave a pattern when there is an attempt to remove the sea. Such pattern sometimes being called a "void".
  - Special adhesives: Which either penetrate the material the seal is affixed to, creating a molecular bond, or two-part adhesives which molecularly bond between the two parts; in either case, the label and package are damaged if removal is attempted.
  - Delamination: A foil material, such as that used for holograms, which delaminates if removal is attempted.
- **Irremovable.** Incapable of being removed.
- **"Visible" refers to an overt security feature**. These features are apparent without additional equipment and can be used by consumers to authenticate tobacco products. Authorities may also use visible elements in the security feature to authenticate the product.
- **"Invisible" refers to a covert security feature**. These features can only be seen using special tools and are, therefore, mainly geared towards enforcement authorities.

7.2. Technical requirements

The technical requirements section aims to describe the different types of security features divided by overt, semi-covert and covert categories.

The analysis also includes an indicative price evaluation and a verification of tax stamps used in the Member States.

The main security feature categories identified are:

- **Overt (visible) –** Authentication element which is detectable and verifiable by one or more of the human senses without resource to a tool, such as colour changing inks, holograms, latent images, watermarks and security threads. Almost always a visible security feature (ISO/IEC 12931:2012, 2012).
- **Semi-covert (visible and invisible) -** Security features requiring limited training to be authenticated.
- **Covert (invisible) –** Authentication element which is hidden from the human senses until the use of a tool by an informed person reveals it to their senses or else allows automated interpretation of the element (ISO/IEC 12931:2012, 2012).
- **Forensic (invisible) -** Forensic markers identified through laboratory analysis.

Please note that the list presented below is a non-exhaustive list of potential security features. As there is a constant evolution of new security features, it may be that new features are developed during the course of this project.

7.2.1. Technical requirements – Overt components

Overt security features can be verified by naked eye (or human senses) without any additional equipment or devices.

The most common overt devices are intended for detection by human sight. These include as examples:

- **Barcode and product coding** - A barcode is a series of vertical printed bars of controlled thickness and separation, representing variable data information in a linear format. A 2D barcode consists of a representation of solid and clear images (usually squares) in a matrix format over a specific two-dimensional structure. Barcodes and code verification services are sometimes marketed as an overt (or "digital") security feature.
- **Hot and cold foil stamping -** Hot and cold foil stamping involves the use of heavy embossing dyes in combination with hot or cold applied foil.
- **Other optically variable devices (OVDs)** - OVDs are visible features with dynamic characteristics that change according to the viewing angle; for example, from one colour to another, or from one image to another. OVDs are similar to holograms but can also include other devices such as image flips or transitions, often including colour transformations or monochromatic contrasts.
- **Security threads and fibres** - Security threads are polyester threads that are either fully or partially embedded down the length of the paper. Fully embedded

threads can only be viewed when the document is held up to the light. Partially embedded threads appear intermittently on one side of the paper. Security fibres are small fibres randomly distributed throughout the paper while it is still in the pulp form. The fibres may be coloured or have fluorescent dyes only visible under UV light.

- **Holograms** - For the purpose of this report, "hologram" refers to any diffractive optical device (DOVD) showing an image or pattern. This can include positive/negative or colour change flip effects which are difficult to replicate.
- **Colour-changing ink -** Inks which change colour when the viewing angle changes, usually by tilting the item on which they are printed. The colour change is usually quite distinctive, with these inks used to create small solid designs, such as logos, which change colour when tilted.
- **Thin films** - Iridescent films made using electro-deposition processes, which have a shimmering effect that can change colour from different viewing angles.
- **Liquid crystal films** - Liquid crystals on a thin film that can appear to switch on or off at different viewing angles to reveal or conceal an image or design, such as a logo or brand name.
- **Guilloche** - An intricate printed pattern of overlapping, continuous coloured lines.
- **Watermarks -** Multi-tone patterns incorporated into paper, seen in transmitted light, so probably not suitable for a label on a tobacco product pack.

There are also overt features for detection by touch, produced using intaglio printing, which puts ink with a noticeable depth to the substrate. These include:

- **Tactility** - Printed lines or patterns sensed by touch as well as vision.

7.2.2. Technical requirements – Semi-covert

Semi-covert security features require a simple tool and minimal training to authenticate, and may also have some elements or partial elements which can also be seen by the naked eye and may at times be incorporated within overt features.

The different types of semi–covert security features are outlined below:

- **Latent images** - Hidden Image Technology (HIT) embeds an image in the print of a product. These effects can be created for detection either by tilting the printed image in a particular manner or by means of using a simple validation device. A latent image detected by means of tilting is created by printing certain elements of the image with a special raised ink. Looking directly at the printed image, it is not apparent that some ink elements are slightly raised compared to others, but as the printed image is tilted and viewed at an angle, the raised ink becomes apparent, obscuring the non-raised printed elements to create a visual effect.
- **Security inks**
    - Thermochromic inks: Inks that change colour when exposed to a change in temperature (hot or cold).

- Photochromic inks: Inks that change colour when exposed to a UV light source.
- Up-converting or down-converting inks: These inks are colourless and transparent in normal lighting conditions but contain a fluorescent ink that emits light when exposed to UV or infrared (IR) light.
- Metameric inks: Inks that appear differently according to the light source. For example, under normal light two items appear identical, but when using a filter or other special illumination the colours on the items appear different.
- Coin reactive/scratch-off inks: The image printed with these inks is white or transparent. The image is revealed when the edge of a coin is rubbed over the ink.

- **Symbolic codes** - Printed symbolic codes, such as QR or 2D barcodes, usually human-visible but requiring an instrument to decode; may be printed in security ink or themselves encoded to deter simple copying and reproduction.
- **Opto-digital** - Optical structures, usually within a DOVD, read by an opto-digital processing system, such as the camera on a smartphone (sometimes through a magnifying lens attached to the phone), which compares the optical characteristics of the hidden content with a reference record.

7.2.3. Technical requirements – Covert components

Covert security features can be authenticated only by using dedicated and specialised electronic readers for authentication.

- **Digital watermarks -** Digital data embedded directly within video, audio or print content which is imperceptible to humans but readable by computers. The watermark may be embedded by means of subtle variations in colours, patterns or applied materials (such as varnish applied to printed material). Digital watermarks may also have parts that are perceptible to the naked eye, although full authentication requires additional specialised equipment.
- **Radio frequency identification device (RFID)** - RFID's are small microchips containing, or able to contain, unique and individual information related to the item to which the chip is attached. They can typically be detected at distances ranging from a few millimetres to several meters. RFID devices may be either active or passive in nature with the active devices emitting RF energy, while passive RFID devices are "interrogated" by active RF signals. These devices are now so small that they can be neatly implanted into plastic cards or paper.
- **Security inks**
  - Magnetic inks: These inks contain small iron oxide magnetic flakes. The inks have two filmic layers, one carrying an invisible magnetic image and the other an invisible magnetisable layer.
  - Conductive inks: A conductive ink creates a printed object which conducts electricity. These inks allow circuits to be drawn or printed on a variety of substrate materials, from polyester to paper.
  - Biometric inks: Biometric inks contain DNA taggants that can be machine read or react to a reading solvent. This allows for verification of a genuine product.

- **Optical structures** - Contained within a hologram or other DOVD, these are laser readable, polarised or other optically encoded image elements, or a hidden image in liquid crystal film or other thin film.
- **Design features** - Micro- or nano-size characters or designs (such as a logo or shield), scrambled images, or Moiré effects, that can be printed or incorporated into a DOVD; codes or images incorporated into the printed designs that are offset from or otherwise scattered between the dots that make up the printed visible image.
- **Chemical** - Up- or down-converting inks or lacquers (i.e. converting the wavelength of human-invisible illuminating light to reveal fluorescent or luminescent images); polarising ink; up- or down-converting fibres or dots incorporated into a paper or board; spots, dots or larger areas within the substrate that react to temperature change or chemical stimulus.
- **UV-dull paper -** Substrate which is treated to be non-fluorescing under UV light (standard paper is UV bright).
- **Digital tag -** Proprietary mark, usually too small for unaided human vision, incorporated into a printed design, containing product-specific information.
- **Fingerprinting -** Includes semi-covert elements that require specialised techniques to authenticate. Fingerprinting involves making a record of a small area of the surface of a product or its pack, at the micro- or nano-scopic scale using a laser or similar scanning method, converting that record to a graphical or numerical representation so that it can be printed onto the product or pack (including data on the location of the scanned area).

7.2.4. Technical requirements – Forensic

There is a wide range of high-technology solutions which require laboratory testing or dedicated field test kits to scientifically prove authenticity. These are strictly a sub-set of covert technologies, but the difference lies in the methodology required for authentication.

- **Forensic markers/nano-taggants -** Forensic markers are molecular or microscopic particles that can be organic or inorganic in composition and exhibit specific and unique physical, biological, or chemical properties. They can be embedded into different aspects of the security features on a product (e.g., holograms, security threads, etc.). Forensic markers are highly secure, but also may be hard to control in multiple markets.

7.2.5. Technical requirements – Components compatibility

Article 16 of the TPD states the need to have security features on all unit packets of tobacco products placed on the market, as a method to fight illicit trade. According to the Directive, all unit packets of tobacco products placed on the market must carry a tamper-proof and irremovable security feature, composed of visible and invisible elements.

The table below demonstrates examples how different security elements can be combined to generate a fully TPD-compliant security feature. In some cases, the method of application will affect whether the feature is tamper-evident or irremovable (i.e. whether it is applied directly on packages or affixed using a carrier such as a label). In these cases, a partial (◐) classification is applied.

The following table also reflects a price classification of low, medium and high. Please note that the previous provided classifications together with that of the low, medium and high cost indications in this security features chart are estimations based on the expert knowledge of the contractor and expert subcontractors. Firstly, it is important to note that the pricing of security features is considered by the manufacturers / solutions providers to be extremely sensitive proprietary information and as such they are unwilling to share this information. Even knowledgeable experts are also highly constrained by confidentiality requirements and agreements so that only low, medium and high indications are possible. Furthermore, it must be mentioned that significant variations in pricing are possible when governments or other users take up new technologies and solutions (volume and market adoption), while at the same time the usual pricing variability can be even 1 to 5 or more depending upon volumes involved. Thus, in certain situations of higher production volumes, high cost security features could at times move toward the medium cost bracket and medium cost security features could move toward the low cost bracket. Finally, in the case of very low production volumes, there is even the chance that low or medium cost features could move toward higher cost brackets.

Security Features	Tamper -Proof	Irremovable	Printing	Affixing	Other Method	Price Range
Overt (visible)						
Barcode and product coding	◐	◐	●	●		Low
Hot and cold foil stamping	◐	◐		●		Medium/High
Other optically variable devices (OVDs)	●	●			●	High
Security threads and fibres	◐	◐		●		Low
Holograms	◐	◐		●		High
Colour-changing ink	◐	◐	●	●		Medium/High
Thin films	●	●			●	High
Liquid crystal films	◐	◐	●	●		High
Guilloche	◐	◐	●	●		Low
Watermarks	◐	◐	●	●		High
Tactility	●	●	●	●	●	Medium
Semi – Covert (visible/ invisible)						
Latent images	◐	◐	●	●		High
Security inks (Thermochromic, Photochromic, Up-converting or Down-converting, Metameric, Coin Reactive/Scratch-Off)	◐	◐		●		High
Symbolic codes	◐	◐	●	●		Low
Opto-digital	◐	◐		●		High
Covert (invisible)						
Digital watermarks	●	●	●	●	●	Medium
Forensic markers/Nano-taggants	◐	◐	●	●		Medium
Radio frequency identification device (RFID)	◐	◐	●	●		High

Security inks (Magnetic, Conductive, Biometric)	◐	◐	●	●		High
Optical structures	●	●	●	●	●	High
Design features	◐	◐	●	●		Low
Chemical	◐	◐		●		Medium
UV-dull paper	◐	◐		●		High
Digital tag	◐	◐		●		High
Fingerprinting	●	●			●	High

Legend:
Tamper-proof ◐- Subject to the use of anti-tampering materials and/or techniques

Irremovable ◐- Dependent on the materials and/or application method

Printing directly on packages ensures that features are irremovable (or destroyed when removed) and tamper-proof (tamper-evident). To ensure that affixed features also meet these requirements, the following methods can be used:

- Mixing strong and weak elements in the materials (substrates) and bond layers (e.g. the adhesive or method by which the security feature is affixed). The most common method is to use frangible paper. Frangible paper or similar materials have very little internal strength and structural integrity. This makes it extremely difficult to remove such labels in one piece and provides visual evidence that someone has tampered with them.
- Micro cuts/ die cuts in the labels that create a weakness in the materials resulting in damage during attempted removal.
- Soluble or chemical sensitive materials may be included in the substrate that dissolve and stain the security feature should it come into contact with solvents or liquids that may be used during tampering attempts. One example may be to include a chemical that reacts and changes colour in the presence of solvents used by individuals attempting to remove the security feature to reuse on fraudulent packs.

The TPD also anticipates the possibility to combine what is required in Article 16 with the security features currently implemented on the tax stamps or national identification marks used by Member States. Presented below is a list of Member States that use/do not use tax stamps and the indication of the entity responsible for tax stamp production

	MS using affixed tax stamps	**MS not using tax stamps**	**Tax stamps produced by public authority** (Under consultation)	**Tax stamps produced by a third party** (Under consultation)
Austria		●		
Belgium	●		●	
Bulgaria	●			●
Croatia	●			●
Cyprus		●		
Czech Republic	●		●	
Denmark	●			●
Estonia	●			●
Finland	●			

	MS using affixed tax stamps	MS not using tax stamps	Tax stamps produced by public authority (Under consultation)	Tax stamps produced by a third party (Under consultation)
France		●		
Germany	●		●	
Greece	●		●	
Hungary	●			●
Ireland	●			●
Italy	●		●	
Latvia	●			●
Lithuania	●			●
Luxembourg	●		●	
Malta	●			●
Netherlands	●			●
Poland	●		●	
Portugal	●		●	
Romania	●		●	
Slovakia	●		●	
Slovenia	●			●
Spain	●		●	
Sweden		●		
United Kingdom		●		

It is important to note that 23 out of 28 Member States currently apply fiscal marks in the form of tax stamps. Among the five Member States that currently do not have tax stamp programmes, different fiscal marks are used. For example, the UK uses tax marks as opposed to tax stamps. Products that carry a fiscal mark also carry a covert anti-counterfeit mark, which is added during the manufacturing process.

7.3. Operational requirements

The operational requirements are divided into two subsections – operational management requirements and rules for size and placement of the security features – with the objective of promoting cooperation between manufacturers, importers and Member States.

7.3.1. Operational management requirements

To maximise the utility of the security features, different considerations related to controls, security, cooperation between manufacturers and Member States, and ease of enforcement/ authentication are outlined below.

1. Security features selection – Member States are responsible for the selection of the different types of security features to be integrated on the tobacco

products depending on the requirements of the Member States and the type of tobacco product considered.

2. Production of security features – Security features can be produced by the Member State or by a third party nominated by the Member State.
3. Security features information exchange – Member States and the European Commission should cooperate and exchange information to ensure adequate enforcement of their security features as outlined in Article 23 of the TPD.
4. Security features confidentiality – All stakeholders involved in the integration of the security features on the production line (e.g. printing house) are responsible for keeping confidential the information regarding the manufacturing process and the security elements. According to ISO 14298:2013 on the management of security printing processes (ISO/IEC 14298:2013 - Graphic technology, 2013), there should be a security printing management system for security printers.
5. Security features security – Customs offices should be responsible for monitoring the security features and ensuring that security features are not compromised along the supply chain, starting with the supplier facilities until the integration of the security features onto the tobacco products.
6. Security features integration – Tobacco manufacturers and importers are responsible for the integration of the security features (by tax stamp, label or direct application on the product) on the tobacco products. However, Member States should conduct regular operational audits in order to help maintain the integrity of the security features.
7. Security features authentication – Member States are responsible for ensuring that security features can be read and tested by the competent authorities.

All stakeholders involved in the security features processes must have transparency vis-à-vis Member States authorities and take the necessary measures to prevent any risk of corruption.

7.3.2. Size and placement rules

According to Article 10 of the TPD, each unit packet and any outside packaging of tobacco products for smoking shall carry combined health warnings. The combined health warnings shall cover 65 % of both the external front and back surfaces of the unit packet and any outside packaging. Packages with combined health warnings must also carry a general warning and information message. Member States may choose to exempt smoked tobacco products other than cigarettes, roll-your own tobacco and water pipe tobacco from the requirement for combined health warnings.

Figure 38: Mock-up of a cigarette package under the Tobacco Products Directive

According to a study conducted for the European Commission on *Proposals and technical specifications for the use of warning messages on tobacco packages* (Burson-Marsteller / Smoke Free Partnership, 2016), there is a wide range of different types of packages used for tobacco products. Security features must be applied to packages of various shapes and materials.

Considering the requirements of the TPD (Articles 8 to 12, 14 and 15(1)) and the range of packages available on the EU market, the following considerations on the size and placement of security features should be taken into account:

Size

When designing security features, it is important to consider the wide range of packages to which they must be applied. Security features must be large enough to allow the use of a combination of technologies with at least some elements visible to the naked eye. At the same time, the security feature should not be so large that it is not possible to place on packages or that it interferes with labelling requirements.

Placement

- As indicated in Article 16, the security feature shall be irremovably printed or affixed, indelible and not hidden or interrupted in any form, including through tax stamps and price marks, or other elements imposed by legislation such as health warnings.
- Placement of security features under the clear wrap may provide a level of protection to the security feature during transport.
- For security features that are affixed, it may be useful to apply them in such a manner that they are destroyed when packages are opened (for both soft and flip-top style packs).
- Allocation of types of security features for authentications in a visible area of the product make quick visual inspections possible.

Some examples of the potential position of tax stamps or other security feature labels on different tobacco products packages are shown in the figure below.

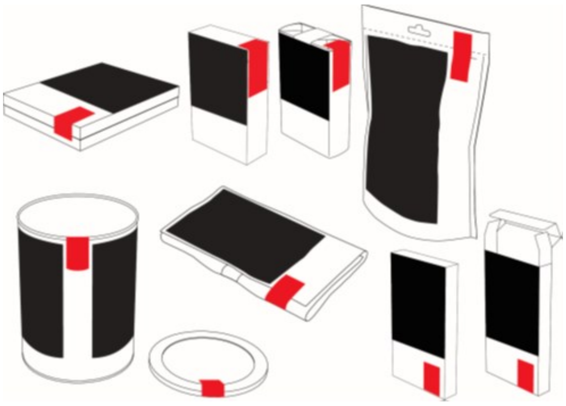


Figure 39: Potential position of tax stamps on smoked tobacco packages[10]

7.4. Rotation Rules

Article 16(2) of the TPD empowers the Commission to lay down rules on the possible rotation of security features.

As part of this Implementation Study, Member States were asked about their current security feature solutions. The initial results show, bearing in mind that this is a highly sensitive area, that:

- Most of the Member States do not have a legal requirement regarding rotation of their security features.
- Security feature are not replaced/rotated at regular intervals but are rather replaced whenever they are believed or found to be compromised.

In general, in order to ensure the authenticity of the tobacco products, it is important to remove or update security features once they have been compromised, and to integrate new hidden security features at regular intervals.

The Feasibility Study (Feasibility Study, 2015) recommends that the security feature be reviewed every three to five years (at minimum every five years) in order to evaluate the integrity of the security elements used to create the security features. This recommendation should also consider the potential costs of updating the security feature, such as redesign, more expensive methods, and additional training for enforcement officials.

[10] (Burson-Marsteller / Smoke Free Partnership, 2016)

8. Glossary and terms of reference

Acronym / Term	Definition
AI	Application Identifier
DSP	Data Storage Providers
EC	European Commission
EMCS	Excise Movement Control System; IT system provided by DG TAXUD to monitor in real-time the movement of excise goods under duty suspension in the EU – manufactured tobacco, alcohol and alcoholic beverages, and energy products
EO	Economic Operators
EPCIS	Electronic Product Code Information Services
ERP	Enterprise Resource Planning
EU	European Union
FCTC	Framework Convention Tobacco Control
GIAI	GS1 Global Individual Asset Identifier
GLN	GS1 Global Location Number
GTIN	GS1 Global Trade Item Number
MS	Member States
OTP	Other Tobacco Products
PM^2	The project management methodology of the European Commission
RYO	Roll Your Own
SEED	System for Exchange of Excise Data; Database for companies to check the validity of an excise number
T&T	Tracking and Tracing
TM	Tobacco Manufacturer
TP	Tobacco Products
TPD	Tobacco Products Directive
UI	Unique Identifier
WHO	World Health Organisation

9. Bibliography

Art 27 Brazilian Law 12402. (n.d.). *Art 27*. Retrieved from http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12402.htm#art5p

ASH. (2015, December 22). *Fact Sheet on the economics of tobacco.* Retrieved January 16, 2017, from http://ash.org.uk/information-and-resources/fact-sheets/the-economics-of-tobacco/

Aung, C. (2013). *Traceability in a food supply chain: Safety & quality perspectives*.

Betts, D., Dominguez, J., Melnik, G., Simonazzi, F., & Subramanian, M. (2013). *Exploring CQRS and Event Sourcing.* Microsoft.

Burson-Marsteller / Smoke Free Partnership. (2016). *Proposals and technical specifications for the use of warning messages on tobacco packages.*

Cognex. (2013). *A guide to barcode symbology for the logistics industry*. Retrieved from http://www.abr.com/wp-content/uploads/2014/08/cognex_wp_expert_guide_symbology_040814.pdf

Cornelis Adrianus van Dorp. (2004). *Reference data-modelling for tracking and tracing*. Retrieved from http://library.wur.nl/WebQuery/wurpubs/fulltext/121536

DG SANCO. (2008). *A study on liability and the health.* Retrieved January 16, 2017, from http://ec.europa.eu/health//sites/health/files/tobacco/docs/tobacco_liability_final_en.pdf

DG SANTE - Tobacco products data dictionary for submission. (2016). *TPD - Submission data dictionary of tobacco products* . Retrieved April 2017, from https://ec.europa.eu/health/euceg/step_by_step_en

Eurobarometer. (2017).

European Comission - Taxation and Costumer Union. (2016). *Excise duty tables*. Retrieved January 16, 2017, from https://ec.europa.eu/taxation_customs/business/vat_en

European Commision - Excise duty tables. (2016). *Excise duty tables.*

European Commision - Targeted stakeholder consultation TPD. (2015, July). *Targeted stakeholder consultation on the implementation of an EU system for traceability and security features pursuant to Articles 15 and 16 of the Tobacco Products Directive 2014/40/EU - DG SANTE*. Retrieved January 16, 2017, from https://ec.europa.eu/health/tobacco/consultations/2015_tpd_consultation_en

European Commission - DG REGIO. (2014, December). *Guide to Cost-Benefit analysis of investment projects.* Retrieved January 16, 2017, from http://ec.europa.eu/regional_policy/sources/docgener/studies/pdf/cba_guide.pdf

European Commission - Feasibility Study. (2015). *Analysis and Feasibility Assessment Regarding EU systems for Tracking and Tracing of Tobacco Products and for Security Features - DG SANTE.* Final Report. Retrieved December 22, 2016, from http://ec.europa.eu/health/tobacco/docs/2015_tpd_tracking_tracing_frep_en.pdf

European Commission - Inception Impact Assessment TPD. (2016). *Inception Impact Assessment of the Implementing and Delegated Acts under Articles 15(11), 15(12) and 16(2) of the Tobacco*

Products Directive 2014/40/EU. Retrieved December 23, 2016, from http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_sante_694_695_696_ia_da_tpd_en.pdf

European Commission - Public consultation TPD. (2016). *Public consultation on the implementation of an EU system for traceability and security features pursuant to Articles 15 and 16 of the Tobacco Products Directive 2014/40/EU*. Retrieved December 22, 2016, from European Commission > DG Health and Food Safety > Public health > Tobacco > Consultations: http://ec.europa.eu/health/tobacco/consultations/2016_traceability_security_features_en.htm

European Commission - TPD Impact Assessment. (2012). *Directive of the European Parliament and of the Council.* Retrieved December 22, 2016, from http://ec.europa.eu/health/tobacco/docs/com_2012_788_ia_en.pdf

European Commission - TPD Impact Assessment. (2012). *Directive of the European Parliament and of the Council.* Retrieved December 22, 2016, from http://ec.europa.eu/health/tobacco/docs/com_2012_788_ia_en.pdf

European Commission - TPD Inception Impact Assessment. (2016). *Inception Impact Assessment of the Implementing and Delegated Acts under Articles 15(11), 15(12) and 16(2) of the Tobacco Products Directive 2014/40/EU*. Retrieved December 23, 2016, from http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_sante_694_695_696_ia_da_tpd_en.pdf

European Commission - TPD Inception Impact Assessment. (2016). *Inception Impact Assessment of the Implementing and Delegated Acts under Articles 15(11), 15(12) and 16(2) of the Tobacco Products Directive 2014/40/EU*. Retrieved December 23, 2016, from http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_sante_694_695_696_ia_da_tpd_en.pdf

Eurostat. (2015). *Population on 1 January by broad age group and sex.* Retrieved January 16, 2017, from http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=demo_pjanbroad&lang=en

Eurostat. (2016). *National accounts and GDP.* Retrieved January 16, 2017, from http://ec.europa.eu/eurostat/statistics-explained/index.php/National_accounts_and_GDP

Feasibility Study. (2015). *Analysis and Feasibility Assessment Regarding EU systems for Tracking and Tracing of Tobacco Products and for Security Features - DG SANTE.* Final Report. Retrieved December 22, 2016, from http://ec.europa.eu/health/tobacco/docs/2015_tpd_tracking_tracing_frep_en.pdf

GS1. (2015). *GS1 Barcode Fact Sheet*. Retrieved from http://www.gs1.org/docs/barcodes/GS1_Barcodes_Fact_Sheet-Scanner_enviroments_and_printing_methods.pdf

ISO/IEC 12931:2012. (2012). *Performance criteria for authentication solutions used to combat counterfeiting of material goods.*

ISO/IEC 14298:2013 - Graphic technology. (2013). *Graphic technology - Management of security printing processes*. Retrieved May 2017, from https://www.iso.org/standard/54594.html

ISO/IEC 19505-1:2012 UML. (2014, April). Information technology -- Object Management Group Unified Modeling Language (OMG UML). Retrieved January 16, 2017, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=32624

ISO/IEC 19987:2015 EPCIS. (2016, December). Information technology - EPC Information services (EPCIS) – Specification. Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66796

ISO/IEC 19988:2015 CBV. (2015, September). *19988:2015 Information technology -- GS1 Core Business Vocabulary (CBV)*. Retrieved January 16, 2017, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66797

Joossens, L., Merriman, D., Ross, H., & Raw, M. (2010). The impact of eliminating the global illicit cigarette trade on health and revenue. *Addiction*(105.9), 1640-1649. Retrieved December 27, 2016

L Ruiz-Garciaa; G. Steinbergerb; M. Rothmundc. (2010). *A model and prototype implementation for tracking and tracing agricultural batch products along the supply chain.*

Mark Richards. (2015). *Software Architecture Patterns.* O'Reilly Media Inc.

Michael T. Fisher; Martin L. Abbott. (2015). *The Art of Scalability: Scalable Web Architecture, Processes, and Organizations for the Modern Enterprise, Second Edition.*

OGG - BPMN 2.0. (2011). *Business Process Model and Notation (BPMN) version 2.0 specification*. Retrieved April 2017, from http://www.omg.org/spec/BPMN/2.0/

Peto, R., Lopez, A., Boreham, J., & Thun, M. (2012). *Mortality from Smoking in Developed Countries 1950-2010.* Oxford University Press.

Priyanka Gaur, S. T. (2014). *Recognition of 2D Barcode Images Using Edge Detection and Morphological Operation*. Retrieved from http://www.ijcsmc.com/docs/papers/April2014/V3I4201499b59.pdf

Reed, H. (2010). *The effects of Increasing Tobacco Taxation: Cost benefit and public finance analysis.* Retrieved January 16, 2017, from ash.org.uk.

SAE J-1739 - FMEA Standard. (2009). *Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA)*. Retrieved April 2017, from http://standards.sae.org/j1739_200901/

Swanson, Marianne; Bowen, Pauline; Phillips, Amy Wohl; Gallup, Dean; Lynes, David. (2010, May). *NIST - Contingency Planning Guide for Federal Information Systems*. Retrieved April 2017, from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

TEC-IT. (2017). Retrieved from Barcode Overview: http://www.tec-it.com/en/support/knowbase/barcode-overview/linear/Default.aspx

Transcrime, Joint Research Centre on Transnational Crime. (2015). *European Outlook on the Illicit Trade in Tobacco Products.* Retrieved January 16, 2017, from http://www.transcrime.it/wp-content/uploads/2015/01/Key-Messages-and-Executive-Summary.pdf

University, C. S. (2011). *2D Barcode Information and Guidelines*. Retrieved from http://www.csuci.edu/news/documents/2011-2dbarcodeinfo.pdf

US Department of Health and Human Services. (2004). *The health consequences of smoking.* Retrieved January 16, 2017, from https://www.surgeongeneral.gov/library/reports/50-years-of-progress/full-report.pdf

US Department of State. (2015). *The global illicit trade in tobacco: a threat to national security.* Retrieved December 22, 2016, from https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=0ahUKEwiSsqrT4OPRAhXCzxQKHUpDCxYQFggcMAA&url=https%3A%2F%2Fwww.state.gov%2Fdocuments%2Forganization%2F250513.pdf&usg=AFQjCNEbODp1bMZhkgwYArsy1QB_5Y5T0A&sig2=A32Kh1BaIkjdV5baw

W3C – World Wide Web Consortium. (2017, april 03). Usage Scenarios. Retrieved april 03, 2017, from www.w3c.org

World Lung Foundation. (2015). *Cigarette use globally.* Retrieved January 24, 2017, from Tobacco Altas: http://www.tobaccoatlas.org/topic/cigarette-use-globally

Yourdon & DeMarco. (2017). *IBM Yourdon/DeMarco data flow diagrams methodology*. Retrieved April 2017, from https://www.ibm.com/support/knowledgecenter/en/SS6RBX_11.4.2/com.ibm.sa.process.doc/topics/c_DFDYourdonDeMarco.html

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);

- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries
  (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm)
  or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

EB-02-17-895-EN-N

Publications Office

doi:10.2818/453932