


Out of scope



Pages 2 to 9 were entirely deleted, as they fall outside the scope of the request

Tracking and tracing				Security features
Who?	Where?		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 policy options

Cost-benefit analysis

Illicit tobacco trade has been estimated to account for 11.26% (European Commission - Inception Impact Assessment TPD, 2016) 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.
 - Other economic benefits

Commented [1]: Suggest to use references from quality journal with peer-review. Many very good research papers exist from credible independent sources. At a minimum use 3-5 source references to get a better/more acceptable/neutral balance here.

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

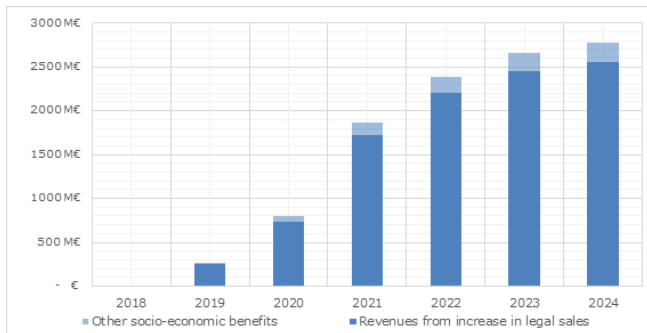


Figure 2: Breakdown of the economic benefits (million €) – Interim Report II

- **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
 - o A percentage of illicit tobacco purchasers will decide to reduce their consumption, or even quit smoking (Transcrime, Joint Research Centre on Transnational Crime, 2015).
 - o 790,000 persons will reduce or quit smoking.
 - Reduction of costs associated with premature mortality due to smoking
 - o 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, 2011).
 - o The decrease in the number of life years lost will reach an estimated total of 114,773 in the European Union.
 - Other social and environmental benefits
 - o Reduction of costs associated with fires caused by smokers' materials.
 - o Improvements in the distribution chain.
 - o Reduction in financing of criminal groups (US Department of State, 2015).

Commented []: Need a specific reference with integrity behind the numbers (sensational sound bite or sound science?)

Commented []: Check grammar and consider a direct quote with reference to page #

Commented []: Could not locate this specific reference, pls double check for accuracy. Found only their previous work from 1950-2000.

Commented []: Reference?

Commented []: References?

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.

	2018	2019	2020	2021	2022	2023	2024
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 ¹	96.97	96.97	96.97	96.97	99.61

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

1.2. 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, 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:

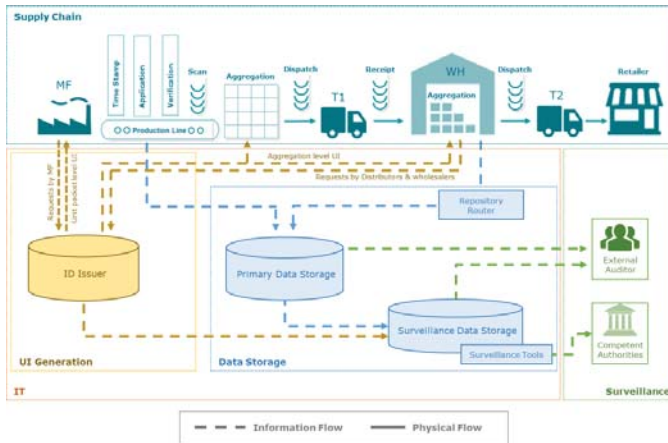


Figure 4: System overview diagram

Commented : ...interacts with raw data and generates information....

Commented : Seems to be missing an 'event' signal for 'receipt' at the retailer? This is a critically important step to ensure supply chain integrity. If not planned now, then this should be on the radar. Ultimately the solution integrity should have a vision of eventually being similar to a pharmacist dispensing as drug with a specialized 2D data matrix scanner (non-point of sale). I know this last reference is not part of the scope but this should be part of the thinking. In this current scenario entrepreneurial retailers can continue to sell illicit with minimum controls – which in mind becomes the weakest link in the system integrity. One option could be to ask industry to step up and do this voluntarily.

¹ The OPEX for 2019 are influenced by the fact that the measure becomes effective in May of that year.

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.

Composition of the unique identifier at unit packet level

Element ID	Information requested	TPD Reference	Code example	Length estimation
UID_1	Place of manufacture	Art 15(2)(a)	A1B2	4
	Manufacturing facility	Art 15(2)(b)		
	Machine used to manufacture the tobacco products	Art 15(2)(c)		
UID_2	Product description	Art 15(2)(e)	C3D4	4
UID_3	Serial number	Art 15(1)	AAE5F6G7H	9
UID_4	Date of manufacture	Art 15(2)(a)	8I9	3
UID_5	Production shift or time of manufacture	Art 15(2)(d)	12	2
UID_6	Intended market of retail sale	Art 15(2)(f)	L2M	3
	Intended shipment route	Art 15(2)(g)		
UID_7	Where applicable, the importer into the EU	Art 15(2)(h)	3N4	3
Total (with verification digit)				29

Commented [1]: The easiest route to implementation is to fully utilize the GS1 system and use numerics only. There should not be an issue in achieving the same result and using non-sequential serialisation codes on a machine should not pose problems for decades even at full speed and non-stop.

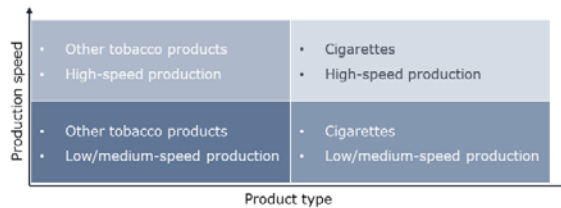
Composition of the unique identifier at aggregation packaging level

Element ID	Information provided	Code example	Length estimation
UID_1	Location of the aggregation activities	A1B2	4
UID_2	Date of the aggregation activities	TD	2
UID_3	Serial number	A1GOE4RT6L	10
Total (with verification digit)			17

• **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 and type of tobacco products



- At aggregation packaging level: Aggregation level



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.




Allowed data carriers at unit packet level

Data Carrier	Characteristics	Example
Data matrix	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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. 	

Commented [JGK10]: Appropriate to reference the ISO and GS1 standards that corresponds. For example, the GS1 standard for QR facilitates GTIN and URL

Commented []: Not entirely correct – the generic QR does not 'carry data' in the same way as the GS1 data carriers as it's a url reroute only. The GS1 QR does carry data and has both the GTIN and URL and hence more secure. China is using QR extensively in payments and it was just reported that one province has USD 50 million in fraudulent payments as crooks place their own QR codes on top of merchants QR.

Allowed data carriers at aggregation packaging level

Data Carrier	Characteristics	Example
Data matrix	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Widely used in logistics operations and can be read by laser scanners. Currently used in the marking of aggregation packaging of tobacco products. 	
QR	<ul style="list-style-type: none"> 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. 	

Human-readable interpretation

This study proposes human-readable interpretation as a complementary measure to increase the robustness of the Tracking and Tracing System. The uniqueness of the code is guaranteed by combining the primary information (machine, date and product description) and the serial number. Consequently, the study proposes a human-readable code that contains the following elements:

Element of information	Code example	Grouping	Grouping example
Machine	34DE	Code 1 – Primary information	34DEEQL5OSG3S
Date	EQT		
Product description	L5OS		
Importer	G3S		
Serial number	11SDF93K2	Code 2 – Serial number	11SDF93K2

Table 3: Elements of information needed for unit packet identification

• Anti-tampering system

The anti-tampering solution should be capable of identifying any unauthorised manipulation of scanning activities in the verification system installed in the manufacturing facilities. 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,

Commented [1]: Please check what the psychologists advise for human readable for numerics and alpha numeric. This is very important.

Commented [2]: May not be the best term as anti-tamper directs the reader to something on a physical product like a seal. Suggest to review the header, maybe something like 'Tamper proofing of the electronic systems' or anti-hacking.

Commented [3]: As above

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 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.

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/importer or a group of specific manufacturer(s)/importer(s). 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.

Commented [1]: Suggest to specify by whom and on what basis

- **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 that 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.

1.3. 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 Governing Body of the Tracking and Tracing System and the tobacco manufacturers and importers of tobacco products.

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. Specifically, 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.

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

Commented : Exchange of information is different from exchange of raw, unstructured data. Key point to ensure consistency throughout the documents, data and information are not interchangeable terms.

as the selection of security features in order to provide guidelines to all entities involved in the process.

In addition, the counterfeit of security features is a widespread problem that affects public authorities, manufacturers, distributors and solution providers. Therefore, this report identifies the different risks associated with the 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).

Commented [1]: Be more specific and describe what is being counterfeited.

Commented [2]: Is there a reference to the statement that can be included?

Commented [3]: Recommend by whom? Can a best practice reference be included?

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).

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 artificially cheap 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.

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 document 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 Commission - Targeted stakeholder consultation TPD, 2015) was to provide stakeholders the option to comment on the Feasibility Study.

The targeted stakeholders were namely 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.

Commented [JGK20]: What does the 'smooth functioning' mean? Smooth is subjective and I suggest to rephrase unless it is commonly used across the EU commission and has an accepted interpretation.

Commented []: Suggest to replace with a less dramatic word such as 'addressing' or similar. Later in the paper there is also inconsistency and 'tackling' is used.

Commented []: Without reference this is speculative and I suggest to replace it with a more neutral term such as 'low cost'

Commented []: Reference available or speculation?

Commented []: I recommend that tracking stops at a 'received' event at retail.

Commented []: Tamper proof versus tamper evident or both?

Commented []: Of course the output is a document but it's an 'extensive review' so I suggest to replace document with 'review'

Commented []: As above, too dramatic, choose alternative word

The Targeted Stakeholder Consultation received 109 responses. The contributions reflect the opinions of all tobacco manufacturers² in the EU and small 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 are in this area.

The Targeted Stakeholder Consultation gathered a great deal of data regarding stakeholder concerns about the options and solutions proposed in the Feasibility Study. They 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.

Commented [redacted] : As above

Commented [redacted] Replace with 'input'

Commented [redacted] Replace with 'These stakeholders'.....

3.1.4. Inception Impact Assessment

In June 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 features
Who? (A) Governance model	Where? (B) Data storage location	How? (C) Allowed data carriers	When? (D) Allowed delays in reporting events	How? (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 4: 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.

² Philip Morris, BAT, JTI, and Imperial

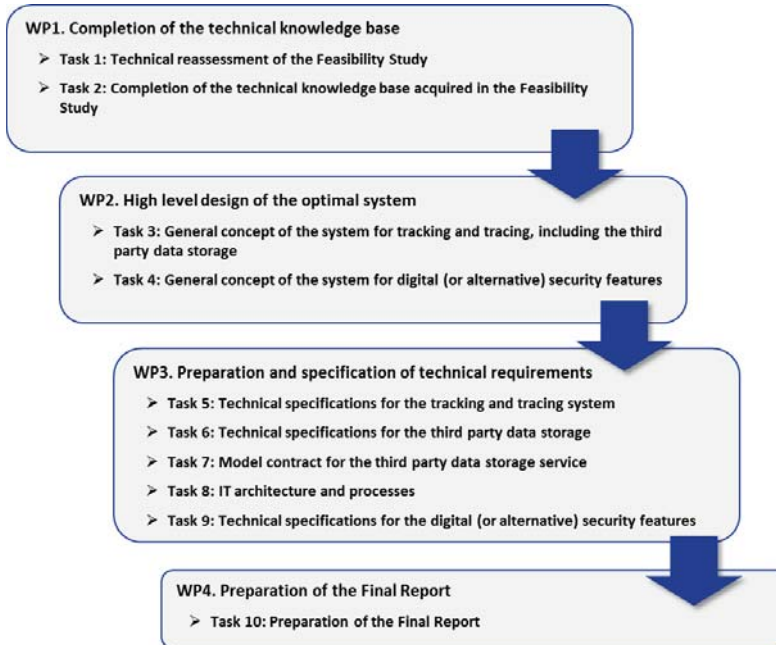


Figure 6: General overview of the Implementation Study Work Packages

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.

Commented [1]: Replace with 'draft'

Commented [2]: Impossible to state 'complete'.....can another word be considered?

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. This resulted in a further review of the cost-benefit analysis 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").

Commented : This appears to be a direct quote requiring a source reference

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 EPCIS through REST.

Commented : First introduction of acronyms require full description and acronym used thereafter

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 7.

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.

Commented : Outline briefly how the selection criteria was defined and determined? Does it reflect a best practice?

Commented : ...based on?

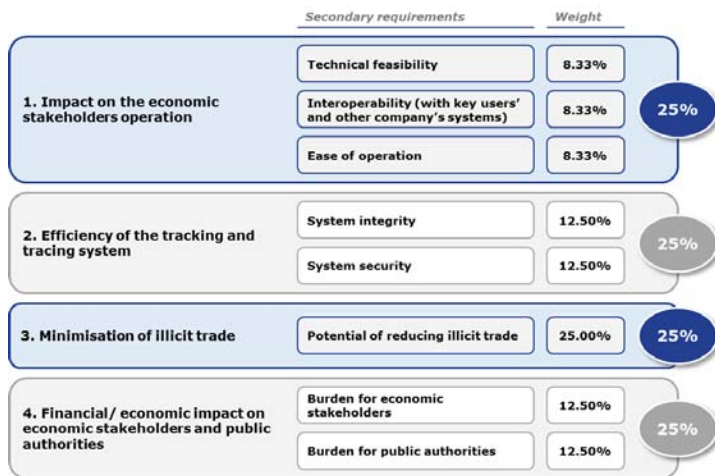


Figure 8: Weighting of the secondary requirements

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

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:

- 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

Commented I don't see 'implementability'. As mentioned several times previously, a solution has a functional view, technical view, implementation view, business or policy view and a standards view. Implementability could be addresses in a survey with stakeholders....this is a critically important aspect. A perfect solution that's not implementable is a bad solution.....implementability is helped by proof of concepts and pilots. Are there plans for both?

(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: 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)

Commented This is a very good addition.

4. GENERAL CONCEPT OF THE SYSTEM

This chapter on the general concept of the System is divided into different sections that aim to provide a clear view 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 acts is conferred to the European Commission by Article 15(11) and 16(2) of the TPD. A

Commented : 'clear view' is subjective, suggest alternative term to describe.

Commented : Earlier references are to 'system', ensure cohesiveness and consistency in terms

Commented : As above

subsidiarity 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.⁴

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.⁵

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.

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.

Commented []: Is subsidiarity the right term usage here ? Reminds of the Catholic social order principles of subsidiarity? Replace with simpler descriptive word or delete

Commented []: This assumes the 'system' is implementable

Commented []: Very optimistic without validation of the entire system through POC's and pilots. Ordering of equipment, onboarding of new business partners that may not be 'friendly', contract negotiations and training of staff are just some of the hurdles and reasons why 70-80% of IT related projects fail. See <https://www.forbes.com/sites/bernardmarr/2016/09/13/are-these-the-real-reasons-why-tech-projects-fail/#57236c6c7320>
http://ibmsystemsmag.com/power/systems-management/workload-management/project_pitfalls/?page=3
<https://www.projectsmart.co.uk/most-it-projects-fail-will-yours.php>

⁴ Judgment of 4 May 2016, *Philip Morris Brands and others* (C-547/14) ECLI:EU:C:2016:325.

⁵ Article 8(2) Protocol.

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.

Commented [redacted]: Not clear.....suggest to refine or replace. Technology for example is only a part of the roll out, the functional changes are significant and include staff and business partner education as well as ordering, testing and implementation of new equipment on production lines. Has anyone checked if ordering of new equipment is needed and if there are constraints by equipment manufacturers such as extended lead times etc.

Commented [redacted]: As mentioned earlier, find an alternative term to anti-tampering to disassociate with AT on the physical product.

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.

Commented [redacted]: system

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.

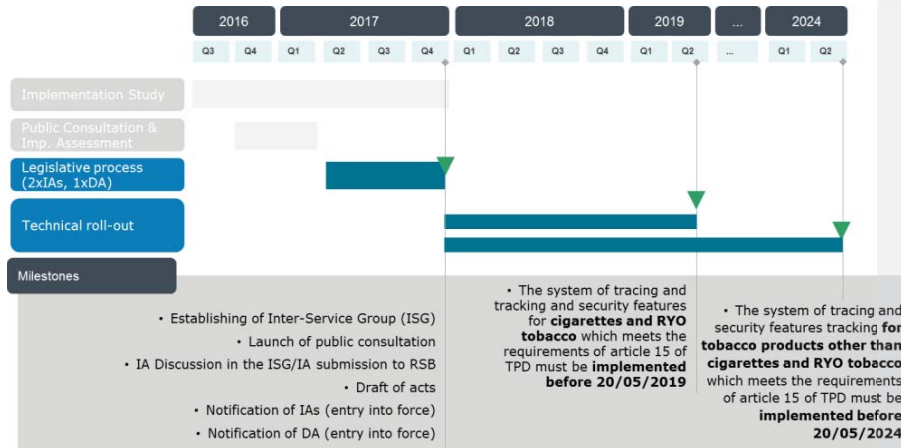
There are also constraints for importers, who have to communicate to their suppliers regarding the need to implement the solutions to mark all unit packets of tobacco products, or mark them by themselves, following the consequent process of aggregation.

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 road map 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.

Commented [1]: system?

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:

Commented [2]: This refers to governance of the system but illicit trade occurs primarily outside of this system. Where are the controls for customs and market surveillance in member states at shop, market and online trade in illicit trade?

	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	<p>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.</p> <p>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.</p>		Contracted by the competent authorities of the Member States, through the entities/agencies with competences on security features.

Commented Does the competent authority have the competency for this role?

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.

Commented: Verify. Usual EU language suggests a definition of economic operators who 'place products on the market'.



4.2. High level solution design

This section presents the high level **solution** 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? (A) Governance model	Where? (B) Data storage model	How? (C) Allowed data carriers	When? (D) Allowed delays in reporting events	How? (S) Method of adding a security feature
(A3) Mixed solution (Industry and third party)	(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	(D1) Near real-time reports	(S3) Mixed solution

Table 8: 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 with minimum disruptions in 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 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.

Commented : Consider dropping 'solution'

Commented : If first introduction, everis needs to be put in context and introduced earlier in the document. Possibly then referred to as the project service provider. Claiming 'everis expertise' opens a can of worms that can be avoided. For example, what is the profile of the expertise and are they full time or hired consultants for the purposes of this report.

Figure 12: 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.

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).

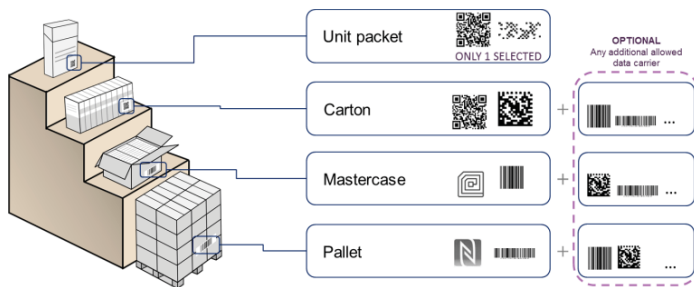


Figure 13. Description of the system with limited variety of data carriers per identification level and optional data carriers for aggregation packaging levels

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 notification 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.

Commented : This should clarify that the 1D data carrier for point of sale purposes with the GTIN is not affected or replaced.

Commented : Use more informative term here instead of notification.....for example 'transmittal'

- A small amount of data sent several times, thereby reducing the volume of data to be sent per transmission, which means a very even and balanced volume of data transmission during a given timeframe.
- The possibility for law enforcement to proactively analyse and react upon a potentially risky event reported.

Commented : Subjective and depends on point of view of system capabilities. Suggest to rephrase or delete.

Commented : Suggest to reword....how is 'risky' defined and where? Are there system triggers for out of tolerance?

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.

Commented : Some member states also solution providers. How does this facilitate / comply with EU anti-competitive behaviour? If a member state is not a solution provider, could they become one to reap the economic benefits rather than non-government solution providers? Will there be open competition or a government led monopoly?

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;

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 10: 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 11: 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%, we can assume that:

- 75.15% of illicit tobacco purchasers would now purchase legitimate tobacco products.

Commented This is too perfect. I think it relies on unrealistic expectations – with no controls at retail, the bad actors will just ship to retail who will sell the cheaper cigarettes. So legitimate tobacco sales may indeed decrease but total volume of cigarettes are likely to continue and fill the void. The model doesn't make sense to me.

- 24.85% of illicit tobacco purchasers would now 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 12: 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 Commission - Taxation and Customs Union, 2016)
(Y): (European Commission - Excise duty tables, 2016)

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

Commented Citation X in Table 13 is incorrect and has spelling errors

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.

Commented: As above, I struggle with these assumptions.

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:

$\text{Decrease in healthcare expenditure (M€)} = \text{Coefficient}_{\text{healthcare}} \cdot \% \text{Reduction tobacco consumption}$

$\text{Increased productivity (M€)} = \text{Coefficient}_{\text{productivity}} \cdot \% \text{Reduction tobacco consumption}$

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 14: 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

Commented: Politically this is fantastic news but practically speaking its unachievable and unconvincing. This requires complex modelling and simulations with many variables that could affect the outcomes. The business case presented lacks rigour and detail.

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 15: 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)	$(K') = (P) \cdot (S) \cdot (I') \cdot (J')$	0.712

Source:
(H') (I'): (Eurostat, 2015)
(J'): (Eurobarometer, 2017)

Table 16: Summary of social benefits I

Commented : As above, plus to validate and verify this is impossible without this report laying out the foundations for a consumer education and enforcement program which is likely not going to happen. Therefore, while it will be difficult if not impossible to implement this report recommendations in line with the timelines, it's non-value added and diversionary to add this information without its own implementation plan tied to SMART goals and objectives.

Commented : If 712,000 people who spend x euro annually on cigarettes quit smoking, then the overall financial benefit should net this out 712,000*x (x=annual spend on tobacco, maybe 1-3 k euro?)

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.

Commented Incomplete argument. Saving lives causes other burdens on society including healthcare costs, food security issues.

Commented Suggest to put references at the bottom of the paragraph.

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	$(M') = (L') \cdot (P) \cdot (S)$	60,274
Monetary value of loss (Millions of euros – Total EU28)	$(N') = (M') \cdot 52,000€$	3,134 M€

Source:
(L'): (DG SANCO, 2008)

Table 17: 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

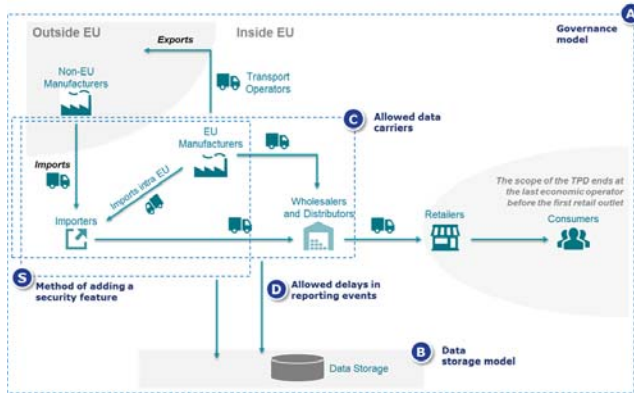


Figure 14: Tracking & Tracing System schema

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
OPEX - Method of adding a security feature	-	9.53	14.30	14.30	14.30	14.30	14.69

Commented : With legislation driving demand and with a finish line in sight, solution providers to tobacco manufacturers can increase prices due to supply and demand balancing and likely add additional worker shifts or outsource if additional and specific equipment is required. As such, a model showing a realistic variance of 20-50% on the CAPEX might need to be considered. A survey or qualitative interviews could help.

	2018	2019	2020	2021	2022	2023	2024
OPEX - TOTAL	-	64.64 ⁶	96.97	96.97	96.97	96.97	99.61

Table 18: Detailed CAPEX and OPEX (Millions of euros) - Interim Report II

4.3.3. Evaluation

The costs of the solution 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.

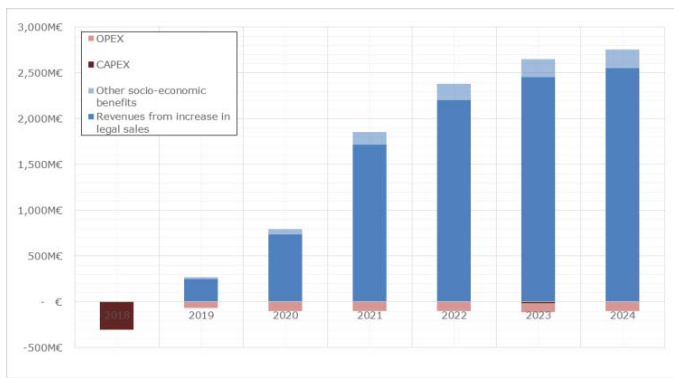


Figure 15: Comparison between the revenues and the costs of the solution (million €)

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.

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.

⁶ The OPEX for 2019 are influenced by the fact that the measure becomes effective in May of that year.

Commented [1]: System

Commented [2]: Likely underestimated when total burden of the 'system' including enforcement is included.

Commented [3]: Speculative at best

Commented [4]: Revenue is overstated and costs understated. This reads like a solution provider sales pitch. Needs to be rationalized and sensitized with the member states. Put simple, of the total revenues, work out the expected percentage of revenue gain for Germany and have a deep dive discussion on where, how and when they will realize the revenue within their contextual framework of operations, enforcement and legislation. I suspect there will be significant surprises. Shouldn't overall revenues start to decline as more smokers quit?

Commented [5]: These references may suggest influence and should be balanced with non-interest group data from reliable sources.

Commented [6]: Revenues may increase for governments but this is speculative and not guaranteed while costs will increase for manufacturers and their trading partners and profit margins will decrease – this is a guarantee. When taken holistically, lowered margins means an inability to invest in innovation to reduce hard and also to maintain or build factories and offices in the member states. So, these number means very little unless taken in the context of the 'total system' include the fully burdened costs of implementing and operating which must include enforcement activities which are not included in the numbers. The data therefore lacks rigour and comes across as poorly justified (lobbyists references) and is akin to a sales and marketing pitch without rigour and defensible substance.

Commented [7]: Benefits for whom? Needs to be specific. For example, will manufacturers sell more tobacco as a result? Will their revenues increase or will their margins increase over time as the system becomes more efficient? How is this measure and by whom?

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:

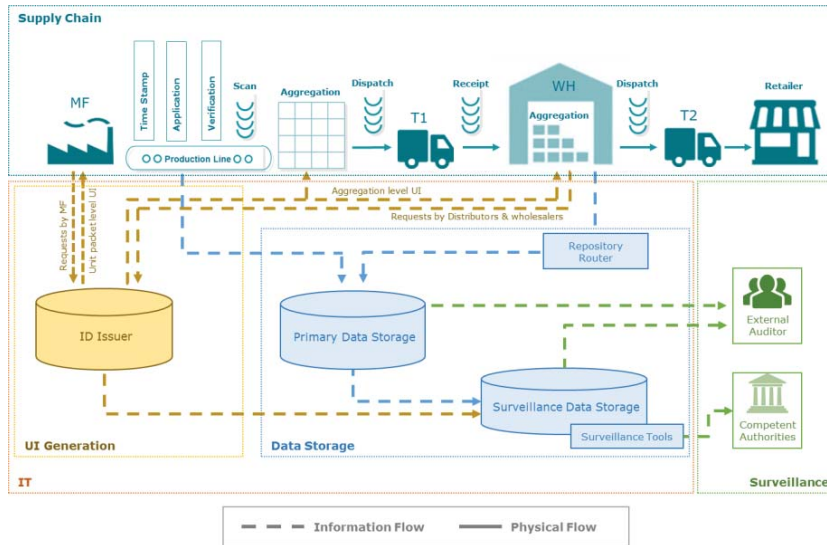


Figure 16: System overview diagram

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".

Commented It should be pointed out that data and information is different and the 'system' requires structured data using standards and regulations to create information that will be shared.

Commented Interacts with data and information

This subchapter on the technical specifications for the Tracking and Tracing System aims to provide a clear view regarding the following:

- 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 data carriers state-of-the-art, 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 protected object 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	System for the issuance of unique identifiers
2.4	Data carrier at unit packet level
2.5	Data carrier at aggregation packaging level

Table 19: 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 that all unit packets of tobacco products shall be marked with a unique identifier. Additionally, Articles 15(2) and 15(3) require that unique identifiers shall allow determining the following elements of information:

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

Commented: Replace with alternative wording

Commented: Should be clearer on physical objects versus the earlier discussions on anti-tampering of digital objects.

Commented: Pls double check that 'shall' is used versus 'should' or 'must'

TPD Article	TPD Request
15(2h)	Where applicable, the importer into the union
15(1)	Uniqueness of the identifier

Table 20: Directive 2014/40/EU requirements

Since Article 15 requires that ten elements of information shall form part of the unique identifier, certain challenges are posed:

- **Length of the unique identifier.** A code with such a high number of data elements is not a common practice in the industry. 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. Otherwise, the negative impact on high-speed production lines will be significant.
- **Access to legible information** for competent authorities. The elements that form the unique identifier can be previously encoded to reduce the length of the unique identifier. This enhances the use of lookup tables as an instrument to decode and to convert the codes into legible information for competent authorities, increasing the effectiveness of surveillance activities.

Hence, the study conducts a three-step analysis 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 (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 proposes a 29 alphanumeric-digit unique identifier formed by seven groups of information: location of the manufacturing facilities, product description, serial number, date of manufacture, time of manufacture, shipment route information, and the importer into the European Union. Additionally, the unique identifier includes a verification digit that enables checking for errors.

Element ID	Information requested	TPD Reference	Code example	Length estimation
UID_1	Place of manufacture	Art 15(2)(a)	A1B2	4
	Manufacturing facility	Art 15(2)(b)		
	Machine used to manufacture the tobacco products	Art 15(2)(c)		
UID_2	Product description	Art 15(2)(e)	C3D4	4

Commented : Ten 'data elements'then when structured, they become information

Commented : This needs more work. In ISO 15459-4 section 5.2 it states "the identity for individual products and product packages shall not contain more than 50 characters. For efficient use within various AIDC data carrier systems, it is recommended that the number of characters to be coded by one linear bar code should not exceed 20 characters, and number of characters should be kept as short as possible regardless of the permissible maximum of 50 characters"

The main problem the above addresses is the ability to print efficiently. Also when the UI needs to be encoded and printed at the same time, the length significantly impacts the size of the data carrier and also the ability to print the human readable code at high speed. Suggest rework here.

Commented : Needs to be expanded.

Commented : Replace with alternative word

Commented : formatting

Commented : this should be 'data analysis' that is then structured to information

Commented : Has numeric-only been excluded? numeric could dramatically improve the chances of a successful rollout following GS1 and ISO standards. Tobacco sector follows naming convention and likely utilize the GTIN for market specific trade so the GTIN can be linked to 1) brand 2) facility 3) machines (using 00-99) and target market. Has this been explored as an option to simplify the coding?

Element ID	Information requested	TPD Reference	Code example	Length estimation
UID_3	Serial number	Art 15(1)	AAE5F6G7H	9
UID_4	Date of manufacture	Art 15(2)(a)	8I9	3
UID_5	Production shift or time of manufacture	Art 15(2)(d)	12	2
UID_6	Intended market of retail sale	Art 15(2)(f)	L2M	3
	Intended shipment route	Art 15(2)(g)		
UID_7	Importer into the EU (where applicable)	Art 15(2)(h)	3N4	3
Total (without verification digit)				28
Total (with verification digit)				29

Table 21: Coding format of the unique identifier at unit packet level

Consequently, some of the unique identifier's information elements require the establishment of lookup tables. The following table summarises the estimated size of the required lookup tables.

Element ID	Information requested	Realistic size	Maximum size
UID_1	Location of the manufacturing activities	19.13Mb	359Mb
UID_2	Product description	11.64Mb	242Mb
UID_4	Date of manufacture	1.3Mb	1.3Mb
UID_6	Intended market of retail sale	19.3Kb	2Mb
	Intended shipment route		
UID_7	Where applicable, the importer into the EU	134Kb	6.71Mb

Table 22: Summary of the lookup table's size

The unique identifier's elements of information are classified into three groups according to the nature of their generation:

- **Primary information**, required by the ID Issuer from the manufacturer or importer.
 - Formed by four elements of information: machine, date of manufacturing, product description, and importer.
- **Serial number**, generated by an independent ID Issuer.
 - The combination of the primary information and the serial number guarantees the code's uniqueness for each unit packet.
- **Secondary information**, included by the manufacturer.
 - Formed by two elements of information: time of manufacturing and shipment route information.

Commented [1]: data elements

Commented [2]: data

Commented [3]: structured

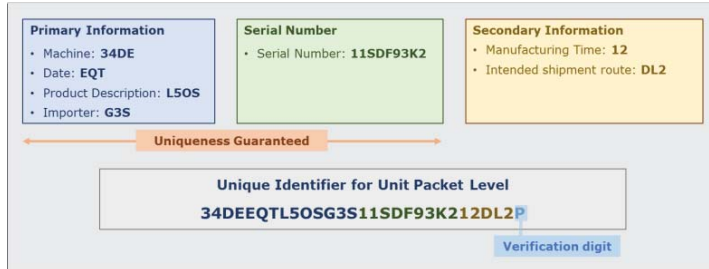


Figure 17: Composition of the unique identifier at unit packet level

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.

When requesting a set of serial numbers, the manufacturers and importers will provide the ID Issuer with the **primary information** (date of manufacturing, location of the manufacturing activities and product description). The generation of serial numbers is further described in the points below.

- Production needs shall not be predictable through the serial numbers. Thus, the ID Issuer shall avoid allocating sequential numbers or predefined ranges of serial numbers.
- The economic operators request a set 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 comprising the following information:
 - Date of manufacturing (e.g. 2021-05-18). This date corresponds to when the unit packet will be manufactured.
 - Location of the manufacturing activities (e.g. 7K53). This information refers to the machine and site of manufacturing, and is maintained through a global lookup table located in the Surveillance Data Storage.
 - Product description (e.g. 9KH). This information refers to the specific SKU of the product to be manufactured on the production line.
 - Importer (e.g. G43). This information refers to the importer of the merchandise into the EU (where applicable).
 - Number of requested serial numbers (e.g. 5,000,000). Quantity of serial numbers to be generated.

Commented: not so sure about the technical requirements to have a trailing verification digit. Can you verify with GS1 or AIDC experts?

Commented: what if the government is the provider? Are there provisions for open competition?

Commented: Wonder why is this term used? Later it refers to batch

Commented: I would prefer to see this described as master data and transactional data.

Commented: Insert word:through the assignment of non-sequential serial numbers.

Commented: Again referring above to 'set' and later to 'batch' the wording is incongruous with the intention. With the suggested addition of the words in the first sentence, the second sentence is redundant

Commented: Insert word: ... economic operators shall request...

Commented: Does this have to be 8 characters versus other shorter and viable options? Figure 18 below has 3 digits for date

Commented: This needs to be expanded with further guidance

Commented: The implementation acts may have to be more specific on whether upper case and/or lower case can be used.

Commented: data

Commented: data

Commented: depending on what is provided, it could be raw unstructured data or information

- o The solution verifies the sender authenticity and the information provided within his/her request.
- o The block of serial numbers is generated according the following rules:
 - Each serial number is random.
 - 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.
- o The ID Issuer notifies the Surveillance Data Storage of the set of serial numbers generated.

Commented [1]: don't like that word here.....system is better

Commented [2]: block or set.....both terms used

Commented [3]: consistency, earlier reference to a set of....

Commented [4]: Check this, I believe non-sequential is a better term than random and the latter may have scalability issues.

Commented [5]: Based on? Is this based on a software program or human interpretation?

Commented [6]: How does the storage as the authoritative source participate in the authentication of the product during its supply chain journey?

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

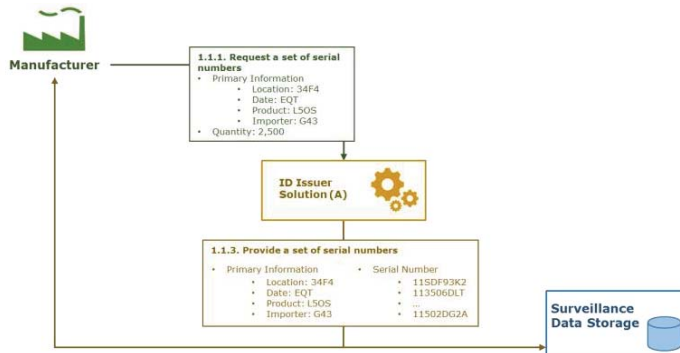


Figure 18: Generation of serial numbers – global view

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. **Readability check.** If the data carrier cannot be read, the unit packet has to be repackaged.
2. **Verifying.** 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:

Commented [7]: Its crucially important to ensure this refers to authenticity of the identifier and not the product. Authenticity of the product cannot be done by means of a security feature, data carrier or tax stamp and can only be verified by forensic methods.

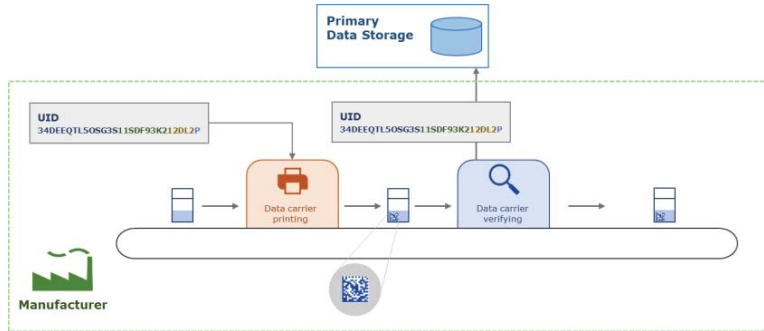


Figure 19: Unique identifier authentication at unit packet level

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 verified by the manufacturer, matches a unique identifier stored in the Surveillance Data Storage under the status "Generated". Additionally, the information contained in the date element of information matches the valid activation date for that unique identifier.
- **Deactivated:** The manufacturer reports the deactivation of that unique identifier. Another cause of deactivation is when a manufacturer tries to activate a unique identifier whose date element of information 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.

Commented: How about 'consumed'? How will this be reported on?

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.

Commented: Can also include cargo theft

- **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.

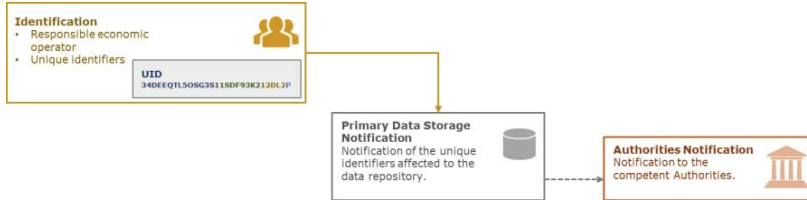


Figure 20: Process for deactivation at unit packet level

5.1.2. Unique identifier (at aggregation packaging level)

5.1.2.1. Composition of the unique identifier at unit packet level

Article 15(5) of the TPD requires the marking and recording of aggregation packages such as cartons, mastercases or pallets. In order to fulfil this requirement, the 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.
- **Similarity with the unit packet unique identifier** to reduce the complexity of the system and enable the use of the lookup tables for the identification of both unit packets and aggregation packaging.

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 of 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

Commented: Be more specific to refer to the GS1 128 or ISO and not confuse with the 1D with GTIN on the pack.

Commented: Consistency – earlier reference to legible. Suggest a better term that both of these.

Commented: Data analysis?

The two-step analysis proposes a 17 alphanumeric digit code that assures uniqueness and is formed by three groups of information: location of the aggregation activities, date of the aggregation activities, and serial number. Also, the unique identifier includes a verification digit that enables checking for errors.

Commented: Nothing is assured or guaranteed. With multiple and uncoordinated solution providers, and without specific mention of GS1 or ISO standards then there is a possibility that data collisions could occur without a controlled and well governed system.

Element ID	Information provided	Code example	Length estimation
UID_1	Location of the aggregation activities	A1B2	4
UID_2	Date of the aggregation activities	A3	2
UID_3	Serial number	AAE5F6G71H	10
Total (without verification digit)			16
Total (with verification digit)			17

Table 23: Example of location of manufacturing activities code

Moreover, two elements of information require 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
UID_2	Date of manufacturing or aggregation	373Kb	48.7Mb

Table 24: Summary of lookup tables size

The unique identifier's elements of information are classified into two groups according to the nature of their generation:

- **Primary information**, required by the ID Issuer from the economic operator.
 - Formed by two elements of information: location and date of aggregation.
- **Serial number**, generated by an independent ID Issuer.
 - The combination of the primary information and the serial number guarantees the code's uniqueness for each unit packet.

Commented: Data?

Commented: data

Commented: no guarantees unless following a globally agreed to convention or standard

Commented: date is 2 characters here



Figure 21: 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 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 European Union legislature.

When requesting a set of serial numbers, the economic operators will provide the ID Issuer with primary information (date of aggregation and location of the aggregation activities). 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 block of serial numbers according to their needs.
- The generation flow is as follows:
 - The economic operator issues a remote request comprising the following information:
 - Date of aggregation (e.g. 2021-05). This date corresponds to when the aggregation occurs.
 - Location of the aggregation activities (e.g. 35FS). This information refers to the facility where the aggregation occurs and is obtained through a global lookup table located in the Surveillance Data Storage.
 - Number of requested serial numbers (e.g. 2,000). Quantity of serial numbers to be generated.
 - 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 random.
 - 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 Surveillance Data Storage of the set of serial numbers generated.

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

- Commented [1]:
- Commented [2]: vitally important to differentiate here between the role of GS1 as the Issuing Agency for globally unique ID and product and brand identify versus the 3rd parties who provide a unique serial number. The serial number issuers must not be seen or utilized as the data or product owner. In this latter scenario, the 'system' must identify the brand owner as the product owner not the UI issuer. If you don't get this right the system will not function.
- Commented [3]: elaborate
- Commented [4]: 'can' versus 'may' or 'should'?
- Commented [5]: this repeats earlier sections.....set of.....batch of consistency needs to be reviewed

- Commented [6]: how?

- Commented [7]: First time introducing a new term.....





Data Carrier	Description	Example
Data Matrix	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 25: 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:

- Manufacturers and importers 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 operators constraints:
 - Ability to scan the selected data carriers

The review of the Stakeholders 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 and the product type – are selected as representatives of the printing conditions for the wide spectrum of tobacco products. These are represented in the following matrix:

Commented : Has any of the team worked in high speed production environments? Its very specific and unique and the line speeds and technologies are very specific.

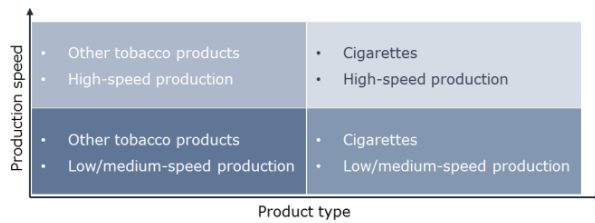


Figure 26: Product type vs production speed matrix

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

Commented [J]: How about small tobacco producers and their constraints?

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.

Commented [J]: What if the solution provider has the DM embedded into their security feature and this creates 2 UIDs on top of the 1D and GTIN at the pack level?




Data Carrier	Characteristics	Example
Data Matrix	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 26: 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 humans 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 elements of information that enable identification of the unique identifier.
- Reduce the length of the human-readable code to improve flexibility of operation and decrease complexity in the printing process.

The uniqueness of the code is guaranteed by combining the primary information (machine, date and product description) and the serial number. Consequently, the Implementation Study proposes the following:

- The human-readable code is comprised of two different-length codes in order to avoid misinterpretation, containing primary information and the serial number.
- The first code contains the primary information merged into a single string (12 characters): the machine, date and product description (in that order).
- The second code contains the serial number (9 characters).

Commented : Which humans? Be more specific here (many different humans.....consumer humans, Regulator humans, enforcement humans)

Commented : How does this tie in with the earlier guidance that the code should not be guessable or predictable etc. ?

Commented : Does 'propose' mean it will be mandatory or a voluntary measure? Be more specific

Commented : Based on what criteria and is this optional or mandatory?

Commented : Caution here. How will the consumer verify the traceability and what forensic tools do consumers have to verify authenticity of the tobacco (contents of the package not the package)? Security features on the outside of the pack cannot verify the authenticity of the contents of the pack.

Commented : Never guaranteed as its not a global system and no formal control mechanisms are being put in place

Element of information	Code example	Grouping	Grouping example
Machine	34DE	Code 1 – Primary information	34DEEQL5OSG3S
Date	EQT		
Product description	L5OS		
Importer	G3S		
Serial number	11SDF93K2	Code 2 – Serial number	11SDF93K2

Table 27: Elements of information needed for unit packet identification

Consequently, the human-readable code is printed along with the data carrier. It distinguishes the primary information and serial number by separating them with a “dash” character or a “line break”.



Figure 27: Examples of human-readable codes associated to data carriers

Commented : It will likely be impossible for modern technology to simultaneously print the data carrier and a 2 line code at speed. Has this been checked with industry? This is likely a major hurdle and defeats the intentions of reducing the burden on stakeholders.

Commented : Impossible for human readability codes like this. There are best practice available on the amount of characters humans can read by number, letter and alpha numeric.

5.1.4. Data carrier (at aggregation packaging level)

5.1.4.1. State-of-the-art analysis

The state-of-the-art 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 carrier], 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 (17 characters).
- The data carrier is not restricted to specific industries or organisations.
- [The code holds specifically a data carrier symbology].
- The data carrier is already implemented in the manufacturing, importing and distributing operations.

Commented : Data not data carrier.....

Commented : This does not make sense...rephrase

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 28: 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

Commented : How about feasibility to implement in scanning equipment in the distribution chain? For example, it would take 7 years for global deployment at scanning of a new data carrier. I am concerned here about the optimism of the feasibility in the distribution chain.

- 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Widely used in logistics operations and readable by laser scanners. • Currently used in the marking of aggregation packaging of tobacco products. 	
QR	<ul style="list-style-type: none"> • 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

The human-readable interpretation refers to the set of characters, such as letters or numbers, which can be read by humans with the aim of identifying the unique identifier without scanners. The addition of human-readable codes is useful in situations where the data carrier cannot be read by a scanning device because it facilitates the deactivation procedure, thereby reducing potential disruptions in the supply chain.

The human-readable code should comply with the following:

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

Commented: Which humans and for what purpose?

- Reduce the length of the human-readable code to improve flexibility of operation and decrease complexity in the printing process.

The uniqueness of the code at aggregation packaging level is guaranteed by combining the primary information (location and date) and the serial number. Therefore, the Implementation Study proposes the following:

- The human-readable code is comprised of two different-length codes in order to avoid misinterpretation, containing primary information and a serial number.
- The first code contains the primary information merged into a single string (6 characters): the location and date (following that order).
- The second code contains the serial number (10 characters).

Element of information	Code example	Grouping	Grouping example
Location	34F4	Code 1 – Primary information	34F4A4
Date	A4		
Serial number	11T7BLO44R	Code 2 – Serial number	11T7BLO44R

Table 29: Elements of information needed for unit packet identification

Subsequently, the human-readable code is printed along with the data carrier. It distinguishes primary information and serial number, by separating them with a “dash” character or a “line break”.



Figure 29: 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

The anti-tampering system is a selection of devices or processes that makes unauthorised access to the protected object easily detected. These measures can either be passive, such as making it difficult to manipulate or obstruct the object; or active, such as tamper-detection techniques, which make a process non-operational if tampered with.

In order to assure the accomplishment of Article 15 of the TPD and to ensure the control of the system by the competent authorities, this report describes and proposes an anti-

Commented : Be more specific...do you mean the cigarette pack or IT system...digital or physical object? If so then say that.

tampering system. This solution is intended to oversee the verification process of the data carriers in the production line.

- The anti-tampering system is operated by an external third party selected by the competent authorities with the objective of increasing the effectiveness of the system and permitting them to identify all potential methods of unauthorised access into a product, package, or system;
- Control or limit the access to products or systems of interest;
- Improve the tamper resistance by making tampering more difficult, time-consuming, etc.;
- Add tamper-evident features to help indicate the existence of tampering.

Then, the anti-tampering system should inform of the occurrence of unauthorised tampering activities in the manufacturing lines of tobacco products by verifying the legitimacy of verification processes. Additionally, it should permit the feasibility and flexibility of operation to reduce the burden for economic operators.

The manufacturer or importer shall not be able 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.

Commented How will the system differentiate an outside hacker motivated by ideological reasons versus illegal attempt to manipulate by the producer?

5.1.5.2. State-of-the-art

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 pharmaceuticals 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.

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:

Commented [1]: Data and information flows

- Temporary Buffer: describes the function of the Temporary Buffer, the component that mediates communication between data sources of the economic operators' proprietary solutions and 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/importer or a group of specific manufacturer(s)/importer(s).
- 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
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 33: Annex II – Chapter 3: Detailed technical specifications for the IT artefacts of the Tracking and Tracing System

5.2.1. Temporary buffer

The Temporary Buffer is an optional component, established on a voluntary basis by the economic operators, that **mediates communication** between data sources of the economic operators' proprietary solutions and the Tracking and Tracing System.

These data events would be collected from an undetermined number of devices from the economic operators (e.g. production lines, scanners, etc.) that send the data to the Temporary Buffer. This component is recommended because it allows the economic operators to decouple the manufacturing and distribution activities from the reporting of events. The Temporary Buffer acts as a **central gateway at a facility level** and is 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 uses a **local storage as an upstream queuing system** for outgoing messages. This local storage acts 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.

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 system 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 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 Temporary Buffers, located at facility level, and are transmitted to the Primary Data Storage through the following data flows:

- Reported directly by the manufacturer(s)/importer(s);
- Routed through the Repository Router of the Surveillance Data Storage solution, which receives the messages from the reporting implementations (e.g. Temporary Buffer component) of 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

Commented : Consistency in terms between solution and system

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 & et al, 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.

Commented [REDACTED]: Inconsistent reference structure suggest (Richards, 2015), Betts et. al, 2013)

Commented [REDACTED]: Betts et al. (2013) not Betts & et al

- 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).

Commented [1]: Use referencing convention such as APA (Fisher & 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 much the same as 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 Repository Router will handle massive amounts of data events because the ID Issuer solutions and the reporting components (a.k.a. Temporary Buffers) 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 durable 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 Temporary Buffer and the Repository Router should use a TCP-based data streaming protocol. The Temporary Buffer, which

Commented: Not a valid comment – handle significant volumes is better but this depends on what is meant by volumes.....and in the context of the system scalability and processing tolerances.

Commented: What is a durable queue? Can you rephrase in simpler terms without jargon

pushes the data to the Repository Router, initiates 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.

Commented : How is resilience to hacking controlled and who monitors it?

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.

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 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

Commented [] : Check this is the ID issuer a 'system'?

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:

- **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

Commented This is important to note that technologies move at a rapid pace and this is an example only for reference purposes.

Commented Barcode is a data carrier so ensure the terminology is consistent throughout the document

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. A covert feature can be created by embedding visual artefacts in the image, which can only be seen with a special optical lens (film overlays such as polarising filters). This lens allows only specific areas of the image to be revealed at any one time. As the inspector moves the filter around and finds the correct alignment, the part of the image containing the hidden digitised image becomes visible. The hidden section scan shows different images as the lens rotates.
- **Security inks**

Commented [10]: It's not a training manual so significantly reduce the text.

- **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. The inks can be coloured or colourless. The authenticity of a product/document with photochromic ink can also be checked by exposure to sunlight or other strong artificial lights. There can also be a hybrid of the thermochromic and the photochromic inks using cold and sun activation.
 - **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. A device emitting light in the necessary spectrum to trigger this effect is required to check that this ink is in place. Laser activated inks are similar, but only change colour when activated by a very specific frequency of 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. This provides for immediate verification of authenticity without the use of special devices.
- **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.

Commented []: As above, reduce....point to authoritative sources

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. Magnetic inks are mainly used for serialisation and numbering purposes but are also found in base security inks within banknotes.
- **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. This can result in optical effects, such as flashing 'lights' or making covert messages appearing when tested.
- **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. These are completely covert but require specialised methods to validate their authenticity. There are optical machine-readable taggants that require a UV/IR light reader – if the wavelength response matches the calibration of reader then the ink is authentic. There are also magnetic based taggants that are a physically-based system, not chemistry-based. A handheld device, similar to an MRI, is used to authentic inks.

Commented []: As above, significantly reduce.

- **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). To authenticate the item, the same area is scanned and the result compared to the result captured in the printed graphic; if they match, the item is genuine. Because at this scale any surface area is unique (hence the name, by analogy to human fingerprints), criminals cannot simply copy the graphic to print on to a counterfeit.

Commented []: reduce

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-tagants** - 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

Commented [1]: does this mean the barcode is not irremovable and not tamper proof? If so this is incorrect on both counts

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-tagants	●	●	●	●		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

Commented [120]: isn't a tactile feature invisible until touched for example?

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	●			
France		●		
Germany	●		●	
Greece	●		●	
Hungary	●			●
Ireland	●			●
Italy	●		●	
Latvia	●			●
Lithuania	●			●
Luxembourg	●		●	
Malta	●			●
Netherlands	●			●
Poland	●		●	
Portugal	●		●	
Romania	●		●	
Slovakia	●		●	
Slovenia	●			●
Spain	●		●	
Sweden		●		
United Kingdom		●		

Commented [1]: Brexit

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 and help tackle illicit trade, 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. Application method of security features – Member States are responsible for the selection of the application method of the security features on the tobacco products.
4. 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.
5. 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.
6. 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.
7. Security features integration – Manufacturers 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.
8. Security features authentication – Member States are responsible for ensuring that security features can be read and tested by the competent authorities.

Commented []: help tackle.....fight.....ensure consistency in terms throughout.

Commented []: EU anti-competition laws? Will it go to tender? Will it be monopolized for economic gain by a government?