Implementation analysis of a EU system for traceability and security features of tobacco products
Interim Report II

With the high level solution in hands, the general concept of the optimal system is specified through the definition of a set of specific elements. These elements, based on the preliminary results, are the:

- Business Process Diagram;
- Data Flow Diagram;
- Sequence Diagram;
- System Architecture;
- Business Case, and;
- Project Charter.

These concepts will be further detailed on Work Package 3, with the preparation and specification of technical requirements that will enable the definition of the implementing and delegated acts for Articles 15 and 16 of the TPD.
Implementation analysis of a EU system for traceability and security features of tobacco products
Interim Report II

Consumers, Health, Agriculture and Food Executive Agency
Health Programme
2016

manufacture, presentation and sale of tobacco and related products, including traceability
and security features as the measures intended to secure the supply chain. The TPD
facilitates the smooth functioning of the internal market for tobacco and related products,
taking as a base a high level of protection of human health, especially for young people,
while addressing 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 illicit trade in tobacco products and thus, from
a public health perspective, contribute to reducing the artificially cheap supplies of illegal
tobacco products that affect the uptake and general prevalence of smoking. Article 15 of
the TPD requires that tobacco products must be tracked and traced. For this to be achieved
it is required that all unit packets of tobacco products manufactured in or imported into the
European Union are marked with a unique identifier (containing defined data elements)
and that their movements are recorded throughout the supply chain (up to the last level
before the first retail outlet). In addition to tracking and tracing, Article 16 of the TPD
requires that all unit packets of tobacco products, which are placed on the EU market, carry
a tamper proof security feature composed of both visible and invisible elements.

2.1.2. Feasibility Study

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

The Feasibility Study is a thorough and extensive document with a high degree of detail
encompassing the main components of a future track and trace solution for the EU, where
the overall foundation of the study was based upon 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 requirements of multiple stakeholders;
- Possible alternative Options for both tracking and tracing and security features;
- Benchmarking with existing track and trace systems currently in operation.

2.1.3. Targeted Stakeholders Consultation

The objective of the Targeted Stakeholders Consultation was to provide the stakeholders
with a possibility to comment on the Feasibility Study.

The targeted stakeholders, namely manufacturers and importers of finished tobacco
products, wholesalers and distributors of finished tobacco products, providers of solutions
for operating traceability and security features systems, and governmental and non-

3 Analysis and Feasibility Assessment Regarding EU systems for Tracking and Tracing of Tobacco Products and
4 All 110 responses to the targeted stakeholder consultation are available at:
governmental organisations active in the area of tobacco control and fight against illicit trade, were advised to review the Feasibility Study before responding to this consultation, which was online from the 7th of May 2015 to the 31st July 2015.

The Targeted Stakeholders Consultation managed to receive, analyse and review 110 responses from stakeholders in 25 countries, including countries outside the EU. The contributions reflect the opinions of the “big 4” tobacco manufacturers\(^5\) in the EU and small manufacturers of cigars and OTP, international supply chain managers and local distributors, large scale service providers and niche market players, NGOs active in the fight against smoking related health outcomes and illicit trade in tobacco products and lobbyists protecting the interests of the tobacco industry, governmental organisations, and others – essentially all parties affected by changes in tobacco policy. Both the large turnout and the detailed nature of the comments received highlight how important the stakes are in this subject.

The targeted stakeholder consultation allowed to gather a great deal of data regarding stakeholders' concerns about the options and solutions proposed in the Feasibility Study, and also some recommendations/proposals of their own on how to overcome what are seen as the limitations of the options and solutions proposed.

### 2.1.4. Inception Impact Assessment

In June 2016 an Inception Impact Assessment\(^6\) was published as a first step in the impact assessment process of policy options for establishing and operating of an EU tracking and tracing system of tobacco products at packet level in line with Article 15 of the TPD and as requested by the TPD. This is oriented toward developing and implementing 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.

By developing and implementing a traceability system along with security features, illicit supply will be tackled by facilitating detection mechanisms and supporting European law enforcement and public health entities engaged in combatting illicit trade. It is envisaged that a comprehensive traceability solution will provide traceability and control of the distribution chain and will contribute to the functioning of the Internal Market by establishing a common control infrastructure for legitimate tobacco products\(^3\).

One of the main inputs gathered from the Inception Impact Assessment were the alternative policy options. According to this analysis, there are key decision points that need to be addressed in the process of selecting the best possible solution for the implementation of Articles 15 and 16 of the TPD. The summary of the alternative policy options is presented below.

<table>
<thead>
<tr>
<th>Tracking and Tracing</th>
<th>Security features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who? (A)</td>
<td>How? (C)</td>
</tr>
<tr>
<td>Where? (B)</td>
<td>When? (D)</td>
</tr>
<tr>
<td>How? (S)</td>
<td></td>
</tr>
</tbody>
</table>

\(^5\) Philip Morris, BAT, JTI, and Imperial

According to the Inception Impact Assessment, the blocks of options A, B, C, D, and S are largely independent from each other, and all their combinations should be possible. This way, the optimal solution can combine elements that were found on Options 1 and 2 of the Feasibility Study, for instance, ensuring the compliance with all of the TPD requirements.

### 2.1.5. Public Consultation

The main aim of the Public Consultation\(^7\) was to seek input from the general public and interested parties on the various policy options presented in the Inception Impact Assessment for implementing an EU system for traceability and security features, as required under Articles 15 and 16 of Directive 2014/40/EU (TPD).

The Public Consultation period was from 29 July 2016 to 04 November 2016 and the targeted groups were the general public/consumers of tobacco products; retailers of finished tobacco products; manufacturers of finished tobacco products; wholesalers and distributors of finished tobacco products; providers of solutions for operating traceability, security feature or data storage systems; governmental and non-governmental organisations active in the area of tobacco control and the fight against illicit trade.

Through this consultation, the Commission aimed to gain feedback regarding the relevance and impact that the various policy options outlined in the Inception Impact Assessment would have. In particular it aimed to:

- Gain insight into which policy options are capable of fulfilling the TPD requirements whilst at the same time imposing least burden on stakeholders concerned;
- Gain realistic estimations of the financial impact of the envisaged policy options on stakeholders;
- Gain insight into the impact of the envisaged policy options on SMEs;
- Seek the feedback of consumers regarding aspects of particular relevance for them.

---

\(^7\) Public consultation on the implementation of an EU system for traceability and security features pursuant to Articles 15 and 16 of the Tobacco Products Directive 2014/40/EU

2.2. Implementation Study

2.2.1. Objectives

The Implementation Study for EU Tobacco Traceability (hereafter the ‘Implementation Study’) is to assist the Commission in preparing the Implementing and Delegated acts, which in turn are intended to attend the Commission’s general objectives to:

- Fight trade in illicit tobacco products, which undermine the free circulation of compliant products and the protection provided by tobacco control legislation;
- Create EU systems for tracking and tracing and for security features for all tobacco products at packet level, which are being manufactured in the EU or imported into the EU to be placed on the EU market;
- Provide for the effective implementation of Article 8 of the FCTC Protocol in the EU, and;
- Ensure a minimum level of health protection and reducing accessibility of illegal tobacco products to young people.

Specifically, the Implementation Study aims at assisting the Commission in defining the implementing and delegated acts to:

- Develop and implement an EU tracking and tracing system of tobacco products at 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.

2.2.2. Scope

In addition to the unique identifier referred to in Article 15 (TPD), Member States shall require that all unit packets of tobacco products, which are placed on the market, carry a tamper proof security feature, composed of visible and invisible elements. The security feature shall be irremovably printed or affixed, indelible and not hidden or interrupted in any form, including through tax stamps and price marks, or other elements imposed by legislation.

Member States requiring tax stamps or national identification marks used for fiscal purposes may allow that they are used for the security feature provided that the tax stamps or national identification marks fulfil all the technical standards and functions required under this Article and shall apply to cigarettes and roll-your-own tobacco from 20 May 2019 and to tobacco products other than cigarettes and roll-your-own tobacco from 20 May 2024.

2.2.3. Planning

To reach the proposed goals, the Implementation Study is divided into three Work Packages. The first Work Package, summarised in this Interim Report I, is about the completion of the technical knowledge base acquired in the Feasibility Study.

After having a sound technical knowledge, the second Work Package provides the high level design of the optimal system, which will be specified in detail under Work Package 3.
Implementation analysis of a EU system for traceability and security features of tobacco products

Interim Report II

with all the technical requirements for the implementation of a tracking and tracing system and of security features, as per Articles 15 and 16 of the TPD, respectively.

The figure below shows the different Work Packages, and what is contained in each of them.

WP1. Completion of the technical knowledge base
- Task 1: Technical reassessment of the Feasibility Study
- Task 2: Completion of the technical knowledge base acquired in the Feasibility Study

WP2. High level design of the optimal system
- Task 3: General concept of the system for tracking and tracing, including the third party data storage
- Task 4: General concept of the system for digital (or alternative) security features

WP3. Preparation and specification of technical requirements
- Task 5: Technical specifications for the tracking and tracing system
- Task 6: Technical specifications for the third party data storage
- Task 7: Model contract for the third party data storage service
- Task 8: IT architecture and processes
- Task 9: Technical specifications for the digital (or alternative) security features

Figure 4: General overview of the Implementation Study Work Packages

The first Work Package, already delivered, focused on completing the technical knowledge base acquired in the Feasibility Study. The second Work Package, summarised in this report, is about the high-level design of the optimal system, which will be detailed under Work Package 3, with all the technical requirements for the implementation of a tracking and tracing system and of security features, as per Articles 15 and 16 of the TPD, respectively.

Interim Report II summarises both tasks of Work Package 2. The major inputs for this Work Package are the knowledge gathered during the implementation of Work Package 1, and the information contained in the Inception Impact Assessment.

2.2.4. Outcome of Work Package 1

Work Package 1\textsuperscript{10} aimed at completing the technical knowledge base, setting the baseline for the high-level design of the Tracking and Tracing system.

The first part of the Report focuses on the technical reassessment of the Feasibility Study, where the options proposed for Tracking and Tracing system\textsuperscript{2} and for security features were critically analysed. Regarding Tracking and Tracing, no option covers completely all the requirements for the implementation of Article 15 of the TPD. Therefore, alternative policy options should be considered, as proposed in the Inception Impact Assessment\textsuperscript{11}.

Concerning the security features, a great deal of research was conducted on the Feasibility Study, which contains, generically, all the options for security features currently available on the market. However, this analysis was not transposed into the options proposed, which are all based on an affixed paper stamp.

Given the constraints on both the Tracking and Tracing options and the security features, the cost-benefit analysis presents some limitations, and will be further reviewed on Work Package 2 – High level design of the optimal system.

A major recommendation for the high-level design of the Tracking and Tracing system is the consideration of alternative options, as per the Inception Impact Assessment. The intention of the Inception Impact Assessment is to conduct a new, individual analysis, considering the trade-offs that each option presents (e.g. concerning (B) Data storage location, a decentralised data storage may be easier to implement and maintain, but with a centralised data storage it may be easier to treat information and generate reports).

The second part of the Report focuses on the completion of the technical knowledge base acquired in the Feasibility Study. The research conducted was 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\textsuperscript{12} according to the information required by the TPD. From this sizing estimation, it can be inferred the data carrier standards that can encode the data elements of the unique identifier required by the TPD. Also, it is provided an overview of the current industry trends, such as the utilisation of Blockchain as a storage alternative, and EPCIS through REST.

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 in the "General requirements for software/ hardware/ hosting services" section of requirements related to the communications network performance.

\textsuperscript{10} Interim Report I

2.3. Methodology

2.3.1. Approach

With regard to the definition and scoring, which spans across three levels – alternative policy options, selection criteria, and evaluation criteria – the approach followed is described below.

The image below provides for a high-level view of the approach followed.

![High level view of the approach followed](image)

The following sections detail each point of the approach followed, providing for a better understanding of how Work Package 2 of the Implementation Study, and in fact this report, are organised.

2.3.1.1. Refinement of the options proposed in the IIA

The first step of our approach is the refinement of the options proposed in the Inception Impact Assessment. The options initially proposed by the Commission in June 2016 were used for the Public Consultation open from the 29th July to the 4th November 2016.

However, our analysis and inputs received from stakeholders who participated in the Public Consultation led us to refine some of the decision points in-order to guarantee a clearer definition of each option.

For this analysis, all the decision points were kept as in the IIA. The sum of the decisions taken will compose the high-level system.
From this point, the options proposed in the IIA for the Tracking and Tracing system, namely regarding ‘(B) Data storage model’, and ‘(C) Allowed data carriers’.

On ‘(B) Data storage model’, option ‘(B1) Centralised model’ was kept as such, but what was option ‘(B2) Decentralised model’ is now split into two different options:

- (B2) Decentralised model as per Manufacturer/Importer, and;
- (B3) Decentralised model as per Member State.

Apart from this, and additional option was proposed – ‘(B4) Combined model: centralised for surveillance and decentralised for recording as per Manufacturer/Importer’ – which keeps a first layer decentralised for data recording, as in option ‘(B2) Decentralised model as per Manufacturer/Importer’, and adds a second centralised layer for data monitoring and surveillance.

On ‘(C) Allowed data carriers’ the main options proposed in the IIA were kept, but two options were added, C2 and C4, which propose the use of optional data carriers for aggregation packaging levels.

In the end, the main options under evaluation are as presented below.
Table 4: Refined alternative policy options, based on the Inception Impact Assessment

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

For a clearer understanding, all options are detailed under chapter 3. DEFINITION OF THE ALTERNATIVE POLICY OPTIONS.

2.3.1.2. Definition of the selection criteria

The alternative policy options need to be evaluated, and the first level of the evaluation relies on a set of selection criteria predefined in the tender specification. These criteria, and our understanding of each one of them, is presented below:

- Full compliance with Articles 15 and 16 of the TPD with due regard given to Article 8 of the FCTC Protocol: The option complies with all the requirements established in Articles 15 and 16 of the TPD and Article 8 of the FCTC protocol;
- Technical feasibility: The option is technically feasible and can be implemented throughout the economic operators and public authorities;
- Interoperability (with key users’ and other company’s systems): The option allows for establishing the interoperability between heterogeneous systems of key users (both national and European authorities), and with the systems of the economic operators (e.g. to access information that needs to be included in the data carriers);
- Ease of operation: Once it is implemented, the option is easy to operate by the various stakeholders;

Commented: Ease of operation is not the same as ‘easy to operate’. It refers to many things including available skills, technologies, maintainability, upgradeability etc.
Implementation analysis of a EU system for traceability and security features of tobacco products

Interim Report II

- System integrity: The option performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation of the system;
- System security: The option ensures or implements proper controls of the accesses to all system resources and data;
- Potential of reducing illicit trade: The degree in which the option contributes to the reduction of illicit trade and thereby contributes to a high level of health protection through increased consumption of tobacco products;
- Burden for economic stakeholders: The financial/ economic impact for the economic operators generated by the option;
- Burden for public authorities: The financial/ economic impact for the public authorities generated by the option.

These selection criteria apply to all alternative policy options, which enable a standard comparison and, ultimately, the selection of the optimal high-level solution. To identify the optimal option, however, the selection criteria are added up, with different weights, until a final score by option.

After analysing the possibilities at this level, we decided for grouping the criteria per stakeholder’s impact, with a balanced distribution of the weights across the groups.

For this, we first assessed the affected stakeholders. The requirements of Article 15 of the TPD apply to all products manufactured in and/or destined for the EU market. The envisaged system covers all economic operators involved in the trading of tobacco products, from the manufacturer to the last economic operator before the first retail outlet.

The requirements of Article 16 of the TPD (i.e. to irremovably print or affix a security feature to all unit packets of tobacco products), necessarily apply to the initial stage of the production-distribution chain (i.e. to the manufacturers or other entities responsible for placing the tobacco products on the market).

In addition to the economic stakeholders involved in the supply chain of tobacco products, the impact on service providers and national regulators should be assessed.

In addition, all these stakeholders will be affected in the deployment phase. In addition, there is a broader group of stakeholders, including retailers and consumers, who will be affected once the systems for tracking and tracing and for security features are fully operational.\textsuperscript{10}

The stakeholders referenced in figure 7, however, will be affected differently by each of the selection criteria. For this analysis, we focused on the secondary (or optimization) requirements, which are the ones that will be weighted for the final score. For the primary (or mandatory) requirements, the evaluation is done as comply / not comply with Articles 15 and 16 of the TPD and Article 8 of the FCTC Protocol (in case the options do not comply, they are automatically cast out of the evaluation).

The figure below provides for a high-level impact assessment of each secondary requirements (or selection criteria) on the identified groups of affected stakeholders.

Commented: depersonalize
Commented: replace with deleted or withdrawn or eliminated
The global score of each policy option is obtained by multiplying the score of each selection criteria by its respective weight.

2.3.1.3. Definition of evaluation criteria

The selection criteria, however, are not sufficient to evaluate each alternative policy option with the adequate level of precision. For that purpose, a set of evaluation criteria was defined.

The evaluation criteria are placed below each selection criteria, and are policy option specific. For instance, all alternative policy options will be evaluated with regards to the selection criteria ‘System security’, but the corresponding evaluation criteria that contribute to the scoring are specific and distinct for each option.

![Figure 10: Example of the evaluation criteria for a selection criteria](image)

With this point, the first part of the approach is concluded. The process started with the alternative policy options, and then came down to the selection and evaluation criteria. At this point, all the evaluation parameters are defined, and the scoring process can begin.

2.3.1.4. Scoring of evaluation criteria

The scoring of the evaluation criteria is 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 (or mandatory) requirements, the only applicable scoring options were 0 and 100%, meaning that the option either complies with the mandatory requirements, or does not, being cast out of the evaluation. For the secondary (or optimization) requirements, the full spectrum from 0 through 100% applies.

The scoring of each option in the evaluation criteria defined is accompanied by a detailed justification, which allows the understanding of how each option ranks compared to its peers. This can be found on chapter 7. ANNEX A: DETAILED EVALUATION OF EACH POLICY OPTION.

2.3.1.5. Scoring of selection criteria

After scoring each option in the evaluation criteria, the process of scoring the selection criteria is simply adding their specific evaluation criteria, weighted homogeneously (i.e. if...
a selection criteria has three evaluation criteria, each of their scores will be multiplied by one third).

With this process, the results are now at selection criteria level. This is, it is already possible to see which option ranks better in each selection criteria (e.g. technical feasibility, ease of operation, etc.). The figure below illustrates this process (the scores presented are merely indicative).

![Figure 11: Scoring of selection criteria (illustrative)](image)

### 2.3.1.6. Scoring of each alternative policy option

By combining the scoring of the selection criteria with the weights previously defined, one can reach a total score for each alternative policy option. With this result, we reach the end of the scoring process, having the option that best fits the requirements defined by the Commission in each decision point.

In order to differentiate between the selection criteria and the total score, these two levels of evaluation were performed with different colours – blue and magenta (the scores presented are merely indicative).

![Figure 12: Global scoring of the alternatives for a given policy option (illustrative)](image)

The total score is also represented as a ‘radar’ chart, which enables the positioning of the options against each other, and assess where one can be stronger, or weaker. An example of the radar charts prepared is presented below\(^\text{13}\).

\(^{13}\) The radar charts only contain the eight secondary requirements, because no weighting was defined for the two primary requirements – these function as a Boolean variable, without an optimisation objective.
In order to guarantee the resilience of this score, a sensitivity analysis was performed, testing the effect a change in the weight of each selection criteria would have in the final score.

2.3.2. Structure of the report

The study includes the following main chapters:

Chapter 3 - Definition of the alternative policy options - Refine the alternative policy options defined on the Work Package 1 based mainly from what was defined in the Inception Impact Assessment. Under this document, a set of options was defined per key decision point (i.e. who, where, how and when, for Tracking and Tracing; and how, for Security features).

Chapter 4 - Evaluation of each alternative policy options - Analysis of each alternative policy options, with a use of a set of selection criteria predefined:
- Full compliance with Articles 15 and 16 of the TPD and Article 8 of the FCTC Protocol;
- Technical feasibility;
- Interoperability (with the systems of key users and other company systems);
- Ease of operation;
- System integrity;
- System security;
- Potential of reducing illicit trade;
- Burden for economic stakeholders;
- Burden for public authorities.

Chapter 5 - General Concept of the System - Analysis and evaluation of the general concept of the system in a combination of all the decisions taken in each alternative policy option.
Chapter 6 - Interim Report II major output of Work Package 2 and milestone in the project, with the inclusion of the high level design of the optimal system, which will then be specified during Work Package 3.

Chapter 7 (Annex A) - Detailed Evaluation of each Policy Option

Chapter 8 (Annex B) - Detailed Calculation of the Costs

Chapter 9 (Annex C) - Detailed Calculation of the Benefits

Chapter 10 (Annex D) - General Concept of the System

Chapter 11 (Annex E) - Glossary and Terms and References

Commented: Costs to implement? costs to maintain? Total cost of system(s)? Costs are generally defined as Planning, Designing, Implementing and Maintaining.

Commented: I struggle with this...benefits for whom?
3. Definition of the alternative policy options

The alternative policy options were mainly drawn from what was defined in the Inception Impact Assessment. Under this document, a set of options was defined per key decision point (i.e. who, where, how and when, for Tracking and Tracing; and how, for Security features). Everis analysed these options, and based on its expertise together with and specific knowledge acquired during the course of the previous Work Package 1 report, proposed to refine the alternative policy options in Table 5, which now look as presented below.

<table>
<thead>
<tr>
<th>Tracking and Tracing</th>
<th>Security features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who? (A) Governance model</td>
<td>Where? (B) Data storage model</td>
</tr>
<tr>
<td>(A1) Industry operated solution</td>
<td>(B1) Centralised model</td>
</tr>
<tr>
<td>(A2) Third party operated solution</td>
<td>(B2) Decentralised model as per Manufacturer/Importer</td>
</tr>
<tr>
<td>(A3) Mixed solution (industry and third party)</td>
<td>(B3) Decentralised model as per Member State</td>
</tr>
<tr>
<td>(B4) Combined model: centralised for surveillance and decentralised for recording as per Manufacturer/Importer</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 5: Alternative policy options based on the proposal of the Inception Impact Assessment

Each one of the options presented in Table 5 will be defined and detailed below. The objective is to reach a common understanding of the options under evaluation and that, at the end of chapter 3, no doubts remain regarding the alternative policy options.

With this sound basis, we can then proceed to the evaluation of each alternative policy option, and identify the optimal system.
3.1. Governance model

The first alternative policy approach in the definition of the system is the choice of its governance model, which should ensure the required level of system integrity by the allocation of various responsibilities and functions to operators involved in the supply chain, starting from the manufacturers, and providers of necessary services, e.g. third party data storage providers. This allocation should first of all guarantee the fulfilment of the objectives of the system and, secondly, be done in a cost-efficient manner but without undermining the objectives of the system, and meeting the defined primary and secondary requirements.

The different areas of responsibilities and functions of the governance model at the production sites are represented in Figure 14 the diagram below:

The Inception Impact Assessment proposes three different alternatives for the governance model:

- Option A2: Third party operated solution.
- Option A3: Mixed solution (industry and third party)

---

The proposed options cover the two extremes: (be it a solution operated at all stages by the industry (manufacturers, distributors and wholesalers) or be it a solution operated at all stages by a third party,) and a third option with a mixed approach, where responsibilities and functions are allocated individually to the industry or a third party.

Regarding the allocation of responsibilities and functions, the TPD already defines the individual stakeholders which are responsible for several processes of the system. On the other hand, it is possible to isolate and identify other functions, actions and processes which may be considered integral to the functioning of the system, but for which the TPD and the FCTC Protocol do not assign a clear responsible. These may include:

- The responsibility for generation of the unique identifier for each unit packet of tobacco products.
- The printing or affixing of the unique identifier on the tobacco unit packs.
- The verification of the unique identifier.
- The usage of international recognized standards such as ISO or GS1 for allocation, control, maintenance and interoperability of unique identifiers.

While the TPD and the FCTC Protocol do not explicitly mention the above functions, actions and processes, there are some considerations that need to be taken into account when allocating responsibility for them to the different actors involved in the process. Recital 31 of the TPD indicates the general requirement for the design of the tracking and tracing system, which is the need to ensure its independence and transparency. Another consideration is related to the concept of ‘control’15 of the full system, as required by the FCTC Protocol. It is important to highlight that ‘control’ does not necessarily mean ‘ownership’ of the system. The final configuration must allow the competent authorities to control (supervise and direct the actions or function of) the system, while other actors (industry or third party) may be those actually operating/performing some of the activities needed.

In the following sections, the three alternatives (Options A1, A2, and A3) are explained in detail while keeping in mind the above considerations.

15 Art. 8.2 FCTC Protocol: "Each Party shall establish, in accordance with this Article, a tracking and tracing system, controlled by the Party for all tobacco products that are manufactured in or imported onto its territory taking into account their own national or regional specific needs and available best practice."

16 Art.8.12 FCTC Protocol: "Obligations assigned to a Party shall not be performed by or delegated to the tobacco industry."
3.1.1. Industry operated solution

In this option, the manufacturers and importers are responsible for the processes of generation of the unique identifiers for unit packets of tobacco, the printing or affixing of the unique identifiers for the unit packets of tobacco (2) and the scanning/verification of the unique identifiers (3).

All economic operators involved in the supply chain are obliged by the TPD\(^{17}\) to record and transmit to the data storage all the movements of tobacco products in their possession (4).

Though this option is likely to require fewer technical adaptations on the part of the industry, as it may be possible for the industry to make use of existing systems and infrastructures, the independence and transparency of the system needs to be reinforced by performing adequate controls:

- Active controls would need to be implemented by the competent authorities\(^{18}\) during the processes of the generation of the unique identifiers and the printing or affixing, in order to ensure that all the unit packs of tobacco products are marked and that...

\(^{17}\) Art. 15.5 TPD

\(^{18}\) These additional extensive controls include the full time physical presence of enforcement officers on the manufacturers’ (and importers’) facilities and/or technical solutions that ensure the verification of the marking of all unit packets of tobacco products produced or imported.
the unique identifiers are verified, indeed, unique. These extra controls may undermine the global business case as the burden for public authorities would be substantially higher than in the other options, if at all technically feasible.

- Regardless of the active controls, passive control of the system is also required by means of regular, and random or unannounced audits. These audits are needed across the different alternatives of the governance model.

3.1.2. Third party operated solution

In this option, independent third parties are responsible for the processes of generation of the unique identifiers, the printing or affixing of the unique identifiers on the unit packets of tobacco and the scanning/verification of the unique identifiers.

The reporting of all the movements of tobacco products to the data storage remains under the responsibilities of the industry and the distributors and wholesalers, as obliged by art. 15.5 of the TPD.

Some considerations regarding the independent third parties:

---

19 Art.15.1 TPD: "Member States shall ensure that all unit packets of tobacco products are marked with a unique identifier [...]".

Commented: As above, different concepts involved for dentification of serialized products and tax stamp identifier controls.

Commented: Wondering if economic operators is a more appropriate term to be consistent... please consider.
• Member States must ensure that manufacturers, importers and economic operators involved in the EU trade of tobacco products agree and sign contracts with independent third parties to perform the tasks described above.

• Independence and technical capabilities of the third parties shall be assessed. This assessment would need to be renewed periodically, as it is required that the independency and technical capabilities are maintained in the medium and long term.

• When determining the technical standards for the establishment and the operation of the T&T system, the Commission is invited to include the obligation for the economic operators to conclude contracts with an external auditor to monitor the activities of the independent third parties\textsuperscript{20}. This external auditor could be proposed and paid by the tobacco manufacturers and approved by the Commission.

• It is foreseen that multiple independent third parties are engaged in the process, as it is not feasible that a single entity provides services to all the economic operators in Europe.

• To ensure interoperability among the different independent third parties, their activities must follow open and widely deployed supply chain data standards.

• To avoid the risk of generating unique identifiers that are duplicated, unique prefixes shall be allocated to each of the third parties participating in the system\textsuperscript{21}.

As in the previous alternative, the control performed is twofold:

• Active and continuous control is ensured by the presence of independent third parties in the system. All solution components and cabinets installed and operated by the independent third parties at manufacturers’ and distributors’ premises must be fitted with locks, sensors and seals to prevent access and manipulation by unauthorised parties. The independence of the third parties from the industry is monitored by:
  o The recurrent reassessment of the suitability of third parties.
  o The annual reports submitted by the external auditor on the activities of the third parties providing the service.

• Passive control is covered by the regular audits to the whole T&T system performed by the competent authorities.

This alternative provides a higher level of control and independence of the system compared to the industry-operated solution, without incurring in the heavy burdens to the public authorities to control the system. However, independent third parties need to be granted with permanent access to the facilities of the industry to in order to install and

\textsuperscript{20} Following the framework provided by the TPD for the data storage in art. 15.8.

\textsuperscript{21} This practice is endorsed by ISO 15459 (1-8) – Information technology – Unique Identifiers.
operate and maintain their equipment and maintenance in the production lines of the manufacturers and importers, resulting in a big impact on the operational processes. Contracts need to be developed a strong system of liabilities between the industry and the third independent parties that need to be developed, in order to anticipate potential conflicts in case of interruptions in the production process, breach of contractual duties or negligent behaviour.

3.1.3. Mixed solution (industry and third party)

In this alternative, certain individual processes (for example, the generation of the unique identifiers, the printing or affixing or the visual control of the unique identifier) are done separately by the industry or an independent third party, resulting in a mixed solution.

The main benefit of this alternative is that it may enable certain existing infrastructures to be better utilised. This may and avoid unnecessary duplications of procedures, whilst enabling authorities to exercise the overall control of the system via the allocation of certain critical responsibilities to non-industry actors, including the state agencies and independent third parties. This alternative allows full control of the system with minimum disruptions in the current production process and may aid the implementation of the protocols. An optimal allocation of tasks would be one where processes than can contribute to increase independence of the system (generation of the of the unique identifiers) are allocated to an independent third party (or performed by the competent authorities themselves) and those processes that can make the system more operable or technically more feasible (printing or affixing the unique identifiers, scanning/verification) are assigned to the industry.

Commented: Unverified / unquantified assumption. Rephrase as above

Commented: Consider adding
In the above configuration, the codes for the unique identifiers of tobacco products are generated by an external entity to the industry (independent third party or competent authorities themselves). This way, the codes can only be produced via a central server controlled directly or indirectly (through an independent third party) by a competent authority. To request codes, manufacturers and importers need to register with the central server and only the allocated codes will be authorised to be used in the production.

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 introduce necessary security checks over this process that will provide the competent authorities will full quantity control of the system.

The industry is responsible for in-charge of the operational (hardware) processes of the system (marking all unit packets of tobacco and reporting all the movements to the data storage). The impact on the production lines of the industry is minimised while ensuring full control of the generation of the codes and the unit packets marked.

In case that the generation of the unique identifiers is assigned to an independent third party, the activities of this third party should also be monitored by an external auditor.

The control in this alternative is ensured through:

- Active and continuous control is performed by the generation of the codes by authorised parties only (independent third party or competent authorities). This generation is independent to the industry. Reconciliation between the codes generated and unit packets marked and aggregation levels is done at the data storage level.
- Permanent control is implemented for the scanning/verification of the codes by means of anti-tampering devices installed by an independent third party.
- Passive control is performed by the recurrent audits performed by the competent authorities to the whole system and each specific manufacturer, distributor, retailer and logistics chain operator.

---

22 There could also be room for collaboration between the competent authorities (Member States or government agencies) and a third party for the generation of the unique identifiers. For example, 22 of the 28 Member States have a tax stamp system for cigarettes and, in most cases, it is a government agency working with a third party that is responsible for the tax stamp system.
3.2. Data storage models

The second alternative policy approach in the definition of the system is the choice of its data storage model.

The aim of the data storage is to store all relevant data reported by the economic operators, assure its integrity, and make it accessible to the Competent Authorities for surveillance purposes. To this end, the data storage model should firstly, guarantee the fulfilment of the objectives of the system as required by the TPD and, secondly, be implemented in a cost-efficient manner.

This alternative is referred by the Inception Impact Assessment\textsuperscript{23} as "location" of the data storage. However, this Study refers to this alternative as Data Storage "model" because the concepts analysed for each option are broader than just where the data storage is physically located.

The Inception Impact Assessment proposes two different alternatives for the data storage model: B1) Centralised data storage and B2) Decentralised data storage. However, the decentralised alternative can be further extended by taking into account the different criteria that can be applied to distribute data across repositories (i.e. as per manufacturer/importer or as per Member State). Moreover, a combined model has been evaluated as well, which attempts at integrating benefits from both models: centralised and decentralised.

Hence, the Study assesses the following alternatives of data storage models:

- **Option B1**: Centralised model.
- **Option B2**: Decentralised model as per Manufacturer/Importer.
- **Option B3**: Decentralised model as per Member State.
- **Option B4**: Combined model: centralised for surveillance and decentralised for recording (as per Manufacturer/Importer).

Any of the proposed models must be in a position to fulfil the following requirements of the TPD and the FCTC Protocol:

Legal reference | Requirements related to the data storage
--- | ---
TPD Art. 15(4) | The trade information, required under TPD Art. 15(2)(i)(j) and (k), shall be electronically accessible by means of a link to the unique identifier. 
This information may be known at the time of manufacturing, as such it is reported later to the Data Storage once it has been confirmed by the parties involved.

TPD Art. 15(5) | All economic operators involved in the trade of tobacco products, from the manufacturer to the last economic operator before the first retail outlet, shall record the entry of all unit packets into their possession, as well as all intermediate movements and the final exit of the unit packets from their possession. 
The recording of aggregated packaging such as cartons, mastercases or pallets, may help complying the former.

TPD Art. 15(7) | All economic operators shall transmit the recorded data electronically to a data storage facility.

TPD Art. 15(8)(1) | The manufacturers and importers of tobacco products shall conclude data storage contracts with an independent third party.

TPD Art. 15(8)(1) | The data storage facility shall be physically located on the territory of the Union.

TPD Art. 15(8)(2) | The third party’s activities shall be monitored by an external auditor.

TPD Art. 15(8)(3) | Member States shall ensure that the Commission, the competent authorities of the Member States, and the external auditor have full access to the data storage facilities. 
In duly justified cases the Commission or the Member States may grant manufacturers or importers access to the stored data, provided that commercial sensitive information remains adequately protected in conformity with the relevant Union and national law.

TPD Art. 15(9) | The data stored shall not be modified or deleted by an economic operator involved in the trade of tobacco products.

TPD Art. 15(10) | Member States shall ensure that personal data are only processed in accordance with the rules and safeguards laid down in Directive 95/46/EC.

FCTC Protocol Art. 9(5)(a) | All records shall be maintained for a period of at least four years.

Table 6: Requirements from the TPD and FCTC Protocol that are applicable to the data storage

This Study considers that the Data Storage system shall support that the events transmitted include information not only about the unit packet itself but also about the aggregation levels of packaging (i.e. pack to carton, carton to mastercase, and mastercase to pallet). Although the TPD does not force to support the recording and managing of aggregated levels of packaging, if the Data Storage system supports such capability it can take advantage of the aggregated information that currently is handled by some economic operators. Therefore, if the economic operators are able to report data at some aggregation level, it would imply less volume of data to transmit and store. For instance, if the movements are reported at a mastercase level, only one report would be sent at a mastercase level, which would include information of 500 unit packets as an average (i.e. a mastercase contains 50 cartons, and each carton contains 10 unit packets), which is much less data to transmit than 500 different reports. Nonetheless, the unit packet level will be always tracked because the mastercase level may be broken down at any point in the process.
According to the information needs specified by the TPD, it can be derived that two data categories shall be transmitted and recorded in the Data Storage system, as a minimum:

- **Traceability data**, which includes the following information:
  - The unique identifier of the unit packets, which shall include the elements of information referred in Art. 15(2)(a) to Art. 15(2)(h).
  - The entry, intermediate movements and final exit of all unit packets into the possession of any economic operator involved in the trade of tobacco products, as referred in Art. 15(5). Each shipment movement shall be inform about the date, destination, point of departure and consignee, as referred in Art. 15(2)(i), in order to be able to determine the actual shipment route from manufacturing to the first retail outlet.

- **Trade data**, which is referred in Art. 15(2)(j) and Art. 15(2)(k) as the trade information involved in any transaction (i.e. purchaser, invoice, order number and payment records of all purchasers from manufacturing to the first retail outlet).

These data categories shall be reported as events including time-stamp information, which helps establishing a consistent temporal order on the basis of these time-stamps. This is of paramount importance because the inherent nature of the Tracking and Tracing system is totally distributed, and the transmission of data from the remote sources (i.e. manufacturers, importers, wholesalers or distributors) may not be done in real-time. As such, events may be not received in the Data Storage system in the same temporal order in which they occurred.

Moreover, these data categories shall be based on open and mature event and data sharing standards such as ISO/IEC 19987:2015 EPC Information services. Currently, this standard is being widely adopted by the supply chain industry to share data. This open standard specifies an abstract and extensible data model to exchange supply chain specific data (i.e. events, trade and traceability information). Importantly, this standard does not dictate the design or implementation of any data repository or specific technologies and is based on the EPC Information System (EPCIS) GS1 standard version 1.1.

It should be remarked that the TPD provisions in Recital (31), Art. 15(7) and Art. 15(8) the fact that a data storage system shall be established to store all relevant data and support the Tracking and Tracing system functioning. However, the TPD does not state any further indications about which possible models are preferred to accomplish such storage (e.g. one central data repository or several data repositories). Thus, none of the storage models introduced could be discarded for non-compliance with the TPD.

In the following sections, the four alternatives (Options B1, B2, B3 and B4) are explained in detail.

---

3.2.1. Centralised model

In this model, B1, there is an independent centralised Data Storage system at EU level. The centralised model comprises a single Data Storage system, which shall include all the components needed to realize the capabilities required by the TPD.

The logical components of the centralised model are depicted below:

![Centralised model diagram]

The descriptions of the logical components are as follows:

- **Recording Interfaces.** Group of components aimed at exposing secure interfaces that grant the recording of all relevant data. These components should be designed to respond efficiently in order to minimise the impact on the systems of the economic operators that transmit the tobacco products records. A positive acknowledgement of the message is returned in order to indicate that the message has been successfully accepted. If there is some error or the message is rejected, a negative acknowledgement is returned.

- **Data Management.** Group of components that process data prior to the storage, aimed at ensuring data integrity through the assurance of consistency and accuracy of data. As such, the following integrity constraints are enforced:
  - **Default integrity constraints:** primary keys, entity integrity, foreign key and referential integrity.
  - **Specific integrity constraints:** format compliance, discrepancy between unique identifiers of the unit packets of tobacco products, consolidation of...
Implementation analysis of a EU system for traceability and security features of tobacco products
Interim Report II

re-packaging events, consolidation of reverse logistics information, consolidation of aggregation information, coherence of the logistics information included in the report (e.g. when a reception event is received, check firstly if the dispatch event related to that transaction has been already received and secondly whether it informs about that transaction, etc.), management of information received in a sequence order different from when it occurred (i.e. when the Data Storage system receives an out of date event, the event is stored but will not be consolidated until the missing event arrives), etc. Since many data integrity issues may arise, with different priorities and various potential actions to be carried out (e.g. confirm received data, verify inconsistent logistic information, etc.), it will be necessary to use a flexible notification engine where to configure notifications related to these integrity checks. If data cannot be consolidated because some integrity issues arise, it will be buffered internally, waiting for either an approval or the reception of the missing information.

- **Data Abstraction.** Group of components aimed at providing data access objects to persist and retrieve data. This allows to decouple from the physical data system implementation.

- **Consumer Interfaces.** Group of components aimed at exposing secure interfaces that grant access to fully exploit all relevant data in-order-to obtain a consolidated view of the tobacco products movements, helping in monitoring and conducting enforcement activities. Different means of access to data will be made available (e.g. query tool, semantic search, bulk data extraction, Application Programing Interface (API) to facilitate integration with external systems such as EMCS, SEED or the FCTC global information-sharing focal point system, etc.). The data exposed through these components is retrieved from an indexed data repository.

- **Data Repository.** Group of physical data storage components.
  - The implementation of the physical repositories may follow different strategies to scale and deliver an optimum performance. A best practice for large scale systems is to establish separate physical data storage areas according to the project needs and priorities such as frequency of access (e.g. the more often accessed should be stored in the quicker storage tier), age of data, protection or specific business rules. Therefore, such tiered storage environment can deliver the required combinations of performance, capacity and resilience. As a minimum, two tiers of data are recommended according to current state of play: "hot" tier with low response times and "cold" tier with higher response times. When required, data could be moved between tiers automatically.


26 Amazon webservies (AWS) - Storage and Database best practices http://www.slideshare.net/AmazonWebServices/data203-28463220

Commented: De-jargonise. Suggest not to use or refer to commerical interests (Amazon).
Concerning the management of commercially sensitive information, referred specifically in TPD Recital 31 and TPD Article 15(8), the Data Repository shall allow for a logical or physical segregation to avoid by design and by default the access to other data than those generated by the tracking and tracing system. By establishing a logical or physical implementation of segregation of data, data related to the Tracking and Tracing system is kept "separate from other company related data".

The data retention period is four years as a minimum, as required by the FCTC Protocol.

**Cross Cutting Services.** Group of components aimed at providing cross services such as security, configuration, administration, monitoring, personal data management and notifications.

When having an independent centralised Data Storage system is deployed at EU level, the following considerations should be taken into account:

- This model assumes the tendering, selection and deployment of the independent centralised Data Storage system at EU level. The identification of the entity responsible for the selection and the procedure to be followed must comply with has to be carefully analysed in the light of Article 15 TPD.
  
  - A contract, with this independent third party data storage provider, has to be concluded by each of the manufacturers and importers.
  
  - The independence and technical capabilities of the third party data storage provider, as well as the contracts concluded with the manufacturers and importers, shall be approved by the Commission.
  
  - The facilities of the data storage provider and the data must have to be located within the EU Union.

- This model poses the challenge of being a single point of cyber-attack meaning that, in case of disruption of this central system, the update of information by the industry and all the economic operators within the supply chain would be untracked and untraceable (totally or at least not in real time).

- A high risk of monopoly exists because there is a single data storage provider that establishes the Data Storage system.

- The third party data storage activities shall be monitored by an external auditor, who is proposed and paid by the manufacturers and approved by the Commission.

- This model minimises the administrative burden due to the fact that because having a single system means the following: a) there are less contracts to be monitored and approved in comparison with the decentralised options, b) there is only one number of selection processes, and c) the assessment of auditing reports is limited to only one system.

- The Data Storage system shall be designed to support efficiently the storage and access to all relevant data, taking into account the constraint that the data sizing requirements of the whole Tracking and Tracing system shall be supported by this single system.
Finally, some examples of European systems with a central data repository are listed below:

- **TRACES (TRAde Control and Expert System)**\(^\text{27}\). TRACES facilitates the exchange of information between all involved trading parties and control authorities and speeds up the administrative procedures. TRACES enables the possibility to trace back and forth all the movements of animals, semen and embryo, food, feed and plants.

- The Schengen Information System (SIS)\(^\text{28}\). SIS is a highly efficient large-scale information system that supports external border control and law enforcement cooperation in the Schengen States.

And at an international level, it is worth noting that China’s system for tracing pharmaceutical products\(^\text{29}\), has a central storage model where all the product information and shipment data at all packaging levels is stored.

### 3.2.2. Decentralised model as per Manufacturer/Importer

This model, B2, comprises a group of independent Data Storage systems as per manufacturer/importer, where each storage system hosts data exclusively related to a certain manufacturer/importer, and an independent central Federation Services system at EU level, which offers central services necessary to seamlessly communicate with the decentralised Data Storage systems.

The responsibilities of the independent central Federation Services system are twofold:

- **a)** To implement the communication with the different decentralised Data Storage systems in order to provide a comprehensive view of the tobacco products movements regardless of where data is located.

- **b)** To provide a secure unique point for seamlessly routing event notifications from the distributors and wholesalers to the proper Data Storage system.

This model allows for a Data Storage system to be either exclusive for a single manufacturer/importer or to be shared by a group of distinct manufacturers/importers. Moreover, each Data Storage system is autonomous and manages its own database where solely data related to a specific (or group of) manufacturer(s)/importer(s) is stored.

The logical components of this model are depicted below:

---

\(^{27}\) TRACES (TRAde Control and Expert System) - [http://ec.europa.eu/food/animal/diseases/traces/](http://ec.europa.eu/food/animal/diseases/traces/)


The descriptions of the logical components are as follows:

- **Federation Services system.** It is an independent and autonomous system that includes the following components:
  - **Discovery Service.** It provides a single search access point and a lookup mechanism to discover multiple sources of information based on the product identifier’s prefix. To realise a query request from the Competent Authorities, this component has to forward that query to each of the Data Storage systems, wait for the individual results and merge the collected data. Since the Federation Services system does not store traceability nor trade data, any surveillance inquiry has to be spread at each Data Storage system, unless the query is related to a specific manufacturer.
  - **Service Registry:** It manages the registry of locations of the distributed systems. This connectivity information is stored in an internal database. When a new Data Storage system is established, its location has to be configured in the Service Registry to notify the Discovery Service the availability of a new data source.
  - **Repository Router:** It is responsible of routing the traceability and trade events reported from the distributors and wholesalers to the proper target storage. It aims to provide a secure unique point for seamlessly routing and decoupling the client reporting systems of being aware of the Data Storage systems’ location. From the information included in the message and the storages’ locations managed by the Service Registry, this component is able to identify the destination Data Storage system where to route the message. As a first approach, in this particular model, the decision on
storage location could be based on the following rule: if the unit product has been manufactured within the Union then the manufacturer name will be used, otherwise the importer name will be used.

- **Consumer Interfaces.** Group of components aimed at exposing secure interfaces that grant full access to the traceability and trade data in order to obtain a consolidated view of the tobacco products movements.

- **Data Storage system.** It is an independent and autonomous system that includes the same components as the centralised model, but the data finally stored is solely related to a specific (or group of) manufacturer(s)/importer(s).
  - To be fully compliant with the TPD, the data storage provider that stores data on behalf of multiple manufacturers and importers must:
    - Segregate access to data belonging to different companies, so as to preserve commercially sensitive information of each manufacturer or importer separate (Article 15(8) TPD).
    - Separate data related to Tracking and Tracing system from other data of the same company (Recital 31 TPD).
  - The data retention period is the same as the B1 model, four years as a minimum.

With the aim of minimising requirements of the central Federation Services system, it could be further analysed the possibility that some federation specific services (e.g. Repository Router or Service Registry) were actually provided by the Data Storage systems themselves. This could allow for communication savings to the distributors and wholesalers.

When having an independent decentralised model as per (or group of) manufacturer(s)/importer(s), the following considerations should be taken into account:

- In this model, in addition to the data storage itself, a central Federation Services system is necessary to orchestrate the access to the data spread across the group of Data Storage systems. The following considerations should be noticed:
  - This system shall be established by an independent third party solution provider.
  - This option assumes the tender and selection of the independent central Federation Services system at EU level. The identification of the entity responsible for the selection and the procedure to be followed must be carefully analysed in the light of Article 15 TPD.
  - The independent third party solution provider activities shall be monitored by an external auditor, as occurs with the data storage.
  - A contract, with this single independent third party solution provider, must be concluded by each of the manufacturers and importers.
  - The independence and technical capabilities of the third-party solution provider, as well as the contracts concluded with the manufacturers and importers, shall be approved by the Commission.
• Each Data Storage system is established by an independent third party data storage provider.
  - A specific (or group of) manufacturer(s)/importer(s) will select an independent third party data storage provider and conclude a contract with this provider to establish a Data Storage system. The independence and technical capabilities of the third party, as well as the contracts concluded, must be approved by the Commission.
  - Within each Data Storage system, the independent third party data storage provider activities shall be monitored by an external auditor. Annual reports of the external auditors shall be submitted to the Competent Authorities and the Commission.

• In this model, the risk of monopoly is low because it is expected that several providers will be able to offer implementations of Data Storage systems.

• All the systems involved shall be designed to support efficiently the storage and access to all relevant data, taking into account the constraint that data is actually spread between distributed Data Storage systems. As such, the following considerations should be noticed:
  - The overall availability and efficiency depend upon each individual Data Storage system. Hence, accessibility to data may be affected negatively if some of the individual Data Storage system does not perform properly or is not available.
  - There could be potential cross-storage compatibility problems because each data storage provider implementation may interpret differently the specifications.

• This model implies additional administrative burden, in comparison with B1, due to the fact that having several systems (i.e. with the Federation Services system and a group of Data Storage systems) means the following: a) there are more contracts to be monitored and approved, b) the Commission shall conduct a selection process for the Federation Services system, and c) the assessment of auditing reports includes several systems.

Finally, as international example with a similar storage model, the Brazil’s system for tracking and tracing medications should be mentioned. This system has a storage as per supply chain member where is stored all the product information, movements and shipment data.

3.2.3. Decentralised model as per Member State

This model, B3, comprises a group of independent Data Storage systems as per Member State, where each storage system hosts data exclusively related to a certain country, and an independent central Federation Services system at EU level, which

---

Implementation analysis of a EU system for traceability and security features of tobacco products

Interim Report II

offers central services necessary for seamlessly communicate with the distributed Data Storage systems.

The main difference with the B2 model – decentralised as per manufacturer/importer – is that the criteria used to distribute data between the Data Storage systems is the "Member State". As a first approach, the identification of the reference country for the storage location could be based on the following rule: if it has been manufactured within the Union, then the manufacturing Member State will be used, otherwise the Member State where it is imported will be used.

Since this option also deals with data spread across different Data Storage systems, it becomes necessary, as well as in B2 model, the inclusion of a single Federation Services system that manages the connections with the distributed Data Storage systems in order to either retrieve data or to provide a single routing service to simplify the event notifications to the proper storage.

This model allows for a Data Storage system to be either exclusive for a single Member State or to be shared by a group of distinct Member States. Moreover, each Data Storage system is autonomous and manages its own database where solely data related to a specific (or group of) Member State(s) is stored.

The logical components of this model are depicted below:

The descriptions of the logical components are as follows:

- **Federation Services system.** It is an independent and autonomous system that includes the same components as the Federation Services system in the B2 model, but with the following difference:
The Routing Service component is accessed not only by the distributors and wholesalers, but also by the importers. This is due to the fact that in this model, importers would need to access to different repositories, depending on to which country are importing products. As such, the Routing Service component has support additional workload than the B2 model (i.e. reports from importers).

- **Data Storage system.** It is an independent and autonomous system that includes the same components as the B1 model, but the data finally stored is solely related to products manufactured or imported into a specific (or group of) Member State(s).
  
  - To be fully compliant with the TPD, the data storage provider that stores data on behalf of multiple manufacturers and importers will have:
    
    - Segregate access to data belonging to different companies, preserve commercially sensitive information of each manufacturer or importer separate (Article 15(8) TPD).
    
    - Separate data related to Tracking and Tracing system from other data of the same company (Recital 31 TPD).
  
  - The data retention period is the same as the B1 model, four years as a minimum.

With the aim of minimising requirements of the central Federation Services system or even facilitate the reporting of importers that establish its own Data Storage system, it could be further analysed the possibility that some federation specific services (e.g. Repository Router or Service Registry) were actually provided by the Data Storage systems themselves. This could allow for communication savings to the distributors, wholesalers and importers.

When operating an independent decentralised model as per Member State, the following considerations should be taken into account:

- In this model, in addition to the data storage itself, a central Federation Services system is necessary to orchestrate the access to the data spread across the group of Data Storage systems. The following considerations should be noticed:
  
  - This system shall be established by an independent third party solution provider.
  
  - This option assumes the tender and selection of the independent central Federation Services system at EU level. The identification of the entity responsible for the selection and the procedure to be followed be carefully analysed in the light of Article 15 TPD.
  
  - The independent third party solution provider activities shall be monitored by an external auditor, as occurs with the data storage.
  
  - A contract, with this single independent third party solution provider, be concluded by each of the manufacturers and importers.
  
  - The independence and technical capabilities of the data storage provider, as well as the contracts concluded with the manufacturers and importers, shall be approved by the Commission.

- Each Data Storage system is established by an independent third party data storage provider.
A specific (or group of) Member State(s) will select an independent third party data storage provider and conclude a contract with this provider to establish a Data Storage system. The independence and technical capabilities of the third party, as well as the contracts concluded, must be approved by the Commission.

Within each Data Storage system, the independent third party data storage provider activities shall be monitored by an external auditor. Annual reports of the external auditors shall be submitted to the Competent Authorities and the Commission.

In this model, the risk of monopoly is low because it is expected that several providers will be able to offer implementations of Data Storage systems.

All the systems involved shall be designed to support efficiently the storage and access to all relevant data, taking into account the constraint that data is actually spread between distributed Data Storage systems. As such, the following considerations should be noticed:

- The overall availability and efficiency depend upon each individual Data Storage system. Hence, accessibility to data may be affected negatively if some of the individual Data Storage system does not perform properly or is not available.
- There could be potential cross-storage compatibility problems because each data storage provider implementation may interpret differently the specifications.

This model implies additional administrative burden, in comparison with B2, due to the fact that having several systems (i.e. with the Federation Services system and a group of Data Storage systems, which potentially could be even greater than B2) means:

a) there are more contracts to be monitored and approved, b) the Commission shall conduct a selection process for the Federation Services system, and c) the assessment of auditing reports includes several systems.

Finally, an example of a European system with repositories at Member State level, it should be mentioned the implementation of the Falsified Medicine Directive, whose delegated act requires that each country operates its own repository that will hold serialization data of all the medicine products in its supply chain. The delegated act allows for repositories to serve the territory of only one Member State (namely ‘national repositories’) or the territory of multiple Member States (namely ‘supranational repositories’).

### 3.2.4. Combined model: centralised for surveillance and decentralised for recording as per Manufacturer/Importer

This model, B4, comprises an independent central Surveillance system at EU level and a group of independent Data Storage systems as per manufacturer/importer.

The descriptions of the logical components are as follows:

- **Surveillance system.** It is an independent and autonomous system, which is comprised by the following components:
  - Synchronisation. Group of components that receive data from the Data Storage systems that needs to be synchronised and consolidated with the complete Tracking and Tracing database.
  - Repository Router. Group of components with the same goals as within B2 model.
  - Service Registry. Group of components with the same goals as within B2 model.
  - Consumer Interfaces. Group of components with the same goals as within B1 model.
  - Data Repository. Group of components with the same goals as within B1 model.
  - Alert management. This system sets business rules to determine parameters when protocols such as event submission are non-compliant. Alert management operates as an ‘exception management’ mechanism and optimizes the involvement of competent authorities based on risk.

- **Data Storage system.** It is an independent and autonomous system, which includes the same components as the B2 model but with the following differences:
Consumer Interfaces. Group of components with the same goals as B2 model, but also providing secure synchronisation capabilities with the Surveillance system.

Data Repository. Group of components with the same goals as B2 model.

When having a combined model, the following considerations should be taken into account:

- The central Surveillance system provides a comprehensive traceability view on the basis of the data that has been previously synchronised from the different Data Storage systems.

- In this model, in addition to the data storage itself, a central Federation Services system is necessary to orchestrate the access to the data spread across the group of Data Storage systems. The following considerations should be noticed:
  - This system shall be established by an independent third party solution provider.
  - This option assumes the tender and selection of the independent central Surveillance system at EU level. The identification of the entity responsible for the selection and the procedure to be followed must be carefully analysed in the light of Article 15 TPD.
  - The independent third party solution provider activities shall be monitored by an external auditor, as occurs with the data storage.
  - A contract, with this single independent third party solution provider, must be concluded by each of the manufacturers and importers.
  - The independence and technical capabilities of the third party solution provider, as well as the contracts concluded with the manufacturers and importers, shall be approved by the Commission.

- Each Data Storage system is established by an independent third party data storage provider.
  - A specific (or group of) manufacturer(s)/importer(s) will select an independent third party data storage provider and conclude a contract with this provider to establish a Data Storage system. The independence and technical capabilities of the third party, as well as the contracts concluded, have to be approved by the Commission.
  - Within each Data Storage system, the independent third party data storage provider activities shall be monitored by an external auditor. Annual reports of the external auditors shall be submitted to the Competent Authorities and the Commission.

- In this model, the risk of monopoly is low because it is expected that several providers will be able to offer implementations of Data Storage systems.

- All the systems involved shall be designed to support efficiently the storage and access to all relevant data, taking into account the following constraints:
  - The data sizing requirements of the whole Tracking and Tracing system shall be supported by the central Surveillance system.
There is a potential risk of synchronisation issues due to possible data incompatibilities or integrity inconsistencies due to data that should not have been synchronised.

- This model implies a similar administrative burden as B2, due to the fact that since having several systems (i.e. with the Surveillance system and a group of Data Storage systems) means the following: a) there are several contracts to be monitored and approved b) the Commission shall conduct a selection process for the Surveillance system, and c) the assessment of auditing reports includes several systems.

### 3.3. Allowed data carriers

This analysis aims at describing the allowed set of data carriers that will contain the unique identifier 1) per unit packet and 2) per aggregation packaging level, without selecting any specific data carrier. In order to facilitate the understanding of this section, it has been separated into three sub-sections: identification levels, assumptions and options.

#### 3.3.1. Identification levels

The defined "identification levels", represent the categories that group the unit packet and the aggregation packaging levels.

The definition of the options in this analysis is conditioned by the amount of information required in each "identification level".

![Identification Levels](image)

Figure 22. Description of identification levels

The unit packet is the smallest individual packaging of a tobacco or related product that is placed on the market. The aggregation packaging levels allow for the association of tobacco products facilitating their transportation, management and storage. The three levels of aggregation identified by the TPD are: carton, master case and pallet, although further aggregation levels such as containers could be considered in future analyses.
The unique identifier of the unit packet has been estimated to require a maximum length of 161 characters\textsuperscript{32} in order to contain the information required under Article 15 of the TPD:

- Date and place of manufacturing
- Manufacturing facility
- Machine used to manufacture the tobacco products
- Production shift or time of manufacture
- Product description
- Intended market for retail sale
- Intended shipment route
- If applicable the importer into the Union

Besides, this study proposes that the unique identifiers of unit packet will be previously transformed into encrypted digits to prevent the public visualization of the information contained. Thus, the confidentiality of manufacturers’ operations is assured.

In addition, the TPD requires all economic operators in the supply chain to record the entry of all unit packets into their possession, as well as all intermediate movements and the final exit of the unit packets. This obligation is addressed by the marking and recording of aggregated packaging such as cartons, master cases or pallets, provided that the tracking and tracing of all unit packets remains possible.

The aggregated packaging levels usually contain serialized data carriers (serialized shipping container code or SSCC) to facilitate the logistics activities. This process is mature within the EU and they are established and managed by standards body GS1 (www.gs1.org). Subsequently, GS1 in Europe provides structured guidance including documentation to aid and facilitate implementation by the economic operators. It must be clarified that the identifier for the aggregated packaging levels is conceived as an independent data carrier that contains all the information requested for its unique identification.

The unique identifier for aggregated packaging levels is recorded in the T&T system and it is linked with the UID’s of the items contained in it (parent-child hierarchy). I.e. carton’s UID is linked to the \texttt{40-unit10-unit} packet’s UID contained in it, facilitating its traceability across the supply chain.

\textsuperscript{32} Section 5.1.1.1 of the Interim Report I
3.3.2. Assumptions

The identification of the allowed data carriers should take into consideration:

- For the unit packet: due to space limitations, it could only contain a single data carrier.
- For the aggregated packaging levels: it will be considered that there are no space limitations where several data carriers could be contained.

The uses of the data carrier in the aggregation packaging levels are conceived to facilitate the reporting of the following events:

- Aggregation (a number of several items are grouped and identified with a unique identifier, i.e. ten unit packets are grouped into a carton)
- Disaggregation (the aggregated packaging level is separated into items, i.e. a pallet is separated into 25 master cases)
- Entry, exit and intermediate movements through the whole supply chain.

3.3.3. Options

Based on the conclusion of the Inception Impact Assessment, five alternatives have been identified:

- **Option C1**: System with a single data carrier for all identification levels.
- **Option C2**: System with a single data carrier per identification level and optional data carriers for aggregation packaging levels.
- **Option C3**: System with limited variety of data carriers per identification level.

---

**Commented**: Where is the 100 years coming from? This is important to explain and clarify.
- **Option C4**: System with limited variety of data carriers per identification level and optional data carriers for aggregation packaging levels.
- **Option C5**: Free system allowing any existing approved data carrier.

All the options allow for the inclusion of all the information requested by the TPD at all levels of identification, whereas four of them (C1, C2, C3 and C4) guarantee full interoperability with the systems of key users (i.e. the competent national and European authorities).

### 3.3.3.1. System with a single data carrier for all identification levels

This option considers the same data carrier for the unit packet and all the aggregation packaging levels.

In this alternative, the same data carrier is printed or affixed in all the unit packets of tobacco products and their aggregated levels.

The actions taken in this alternative have major implications for three groups of stakeholders:

- **Manufactures and importers:**
  - They **are in charge of** the printing and affixing activities of the data carriers to the unit packet and the aggregated packages.
  - They **have to** adapt their production lines to include the process of printing or affixing the data carrier. In addition, they **have to** include scanners in their production lines to verify the validity of the codes.

- **Wholesalers and distributors:**

---

34 All the data carriers symbolized in the Figures 9, 10, 11, 12 are only a representation for the better understanding and they are not intended to represent the final selection. Further consideration of available data carriers will be set out in the next work package.
Implementation analysis of a EU system for traceability and security features of tobacco products

Interim Report II

- They are in charge of overseeing the reporting of events of tobacco products along the distribution chain according to the TPD.
- They have to adapt their scanning devices to be able to scan the data carrier included in the aggregated levels.

- Public authorities:
  - They have to be equipped to be able to read the data carriers included in the unit packet and the aggregated levels.
  - As only one data carrier is allowed, the scanning device for Public Authorities will also only have to be able to scan one data carrier (easier to the rest of options).

3.3.3.2. System with a single data carrier per identification level and optional data carriers for aggregation packaging levels

This option considers a single, but potentially different per identification level, data carrier for the unit packet and all the aggregation packaging levels. In addition, it is possible to add any approved data carrier for the aggregation packaging levels to facilitate the reading activities.

![Figure 24. Description the system with a single data carrier per identification level and optional data carriers for aggregation packaging levels](image)

In this alternative, one data carrier is printed or affixed in the unit packets of tobacco products, and one data carrier on each aggregation level. Besides, this option considers the addition of optional data carriers for the aggregation packaging levels, containing the same information as the selected mandatory data carrier.

The actions taken in this alternative have major implications for three groups of stakeholders:

- Manufactures and importers:
  - They are in charge of overseeing the printing and affixing activities of the data carriers to the unit packet and the aggregated packages.
They have to adapt their production lines to include the process of printing or affixing the data carrier. In addition, they have to include scanners in their production lines to verify the validity of the codes.

They can print or affix additional data carriers in the aggregated packages to facilitate the tracking and tracing activities of wholesalers and distributors.

- Wholesalers and distributors:
  - They are in charge of overseeing the reporting of events of tobacco products along the distribution chain according to the TPD.
  - They have to adapt their scanning devices to be able to scan the data carrier included in the aggregated levels.
  - They can adapt their current scanning devices if their suppliers include additional data carriers.

- Public authorities:
  - They have to be equipped to be able to read the data carriers included in the unit packet and the aggregated levels.
  - As only one data carrier is allowed, the scanning device for Public Authorities will also only have to be able to scan one data carrier (easier to the rest of options).

### 3.3.3.3. System with limited variety of data carriers per identification level

This option allows operators to choose between a variety of data carriers for the unit packet and the aggregation packaging levels.

![Figure 25. Description of the system with limited variety of data carriers per identification level](image)

In this alternative, one data carrier, selected from a limited set of allowed data carriers, is printed or affixed per identification level (unit packet and aggregation packaging level).
The actions taken in this alternative have major implications for three groups of stakeholders:

- **Manufactures and importers:**
  - They are in charge of overseeing selecting the data carrier that they are going to print or affixed in the unit packet and in the aggregated packaging levels. We consider that this choice will be made in order to minimize the impact in their manufacturing and distribution chain operations.
  - They are in charge of overseeing the printing and affixing activities of the data carriers to the unit packet and the aggregated packages.
  - They have to adapt their production lines to include the process of printing or affixing the data carrier. In addition, they have to include scanners in their production lines to verify the validity of the codes.

- **Wholesalers and distributors:**
  - They are in charge of overseeing the reporting of events of tobacco products along the distribution chain according to the TPD.
  - They have to adapt their scanning devices to be able to scan the data carriers included in the aggregated levels by their suppliers.

- **Public authorities:**
  - They have to be equipped to be able to read the data carriers included in the unit packet and the aggregated levels.
  - As a variety of data carriers is allowed, the scanning device for Public Authorities will also only have to be able to scan several data carrier (or to have multiple devices to read all of them).

### 3.3.3.4. System with limited variety of data carriers per identification levels and optional data carriers for aggregation packaging level

This option enables the economic operators to choose between a variety of data carriers for the unit packet and all the aggregation packaging levels. The data carriers for each identification level variety may differ. It is also optional to add an approved data carrier for the aggregation packaging levels.
In this alternative, one data carrier, selected from a limited set of allowed data carriers, is printed or affixed per identification level (unit packet and aggregation packaging level). Besides, this option considers the addition of optional data carriers for the aggregated packaging levels, containing the same information as the selected mandatory data carrier.

The actions taken in this alternative have major implications for three groups of stakeholders:

- **Manufactures and importers:**
  - They are in charge of overseeing selecting the data carrier that they are going to print or affixed in the unit packet and in the aggregated packaging levels. We consider that this choice will be made in order to minimize the impact in their manufacturing and distribution chain operations.
  - They are in charge of the printing and affixing activities of the data carriers to the unit packet and the aggregated packages.
  - They must adapt their production lines to include the process of printing or affixing the data carrier. In addition, they must include scanners in their production lines to verify the validity of the codes.
  - They can print or affix additional data carriers in the aggregated packages to facilitate the tracking and tracing activities of wholesalers and distributors.

- **Wholesalers and distributors:**
  - They are in charge of overseeing the reporting of events of tobacco products along the distribution chain according to the TPD.
  - They must adapt their scanning devices to be able to scan the data carriers included in the aggregated levels by their suppliers.
  - They can adapt their current scanning devices if their suppliers include additional data carriers.

- **Public authorities:**
  - They must be equipped to be able to read the data carriers included in the unit packet and the aggregated levels.
  - As a variety of data carriers is allowed, the scanning device for Public Authorities will also only have to be able to scan several data carrier (or to have multiple devices to read all of them).

### 3.3.3.5. Free system allowing any existing approved data carrier

This option enables the use of any previously approved data carrier and it gives to the economic operator’s autonomy to choose the data carrier that better fits their needs. The unit packet only contains one data carrier, whereas the aggregated packaging levels do not have limitation.
In this alternative, one data carrier, selected from a free set of approved data carriers, is printed or affixed per identification level (unit packet and aggregation packaging level). Besides, this option considers the addition of optional data carriers for the aggregated packaging levels, containing the same information as the selected mandatory data carrier.

The actions taken in this alternative have major implications for three groups of stakeholders:

- **Manufactures and importers:**
  - They are in charge of overseeing selecting the data carrier that they are going to print or affixed in the unit packet and in the aggregated packaging levels. We consider that this choice will be made in order to minimize the impact in their manufacturing and distribution chain operations.
  - They are in charge of the printing and affixing activities of the data carriers to the unit packet and the aggregated packages.
  - They have to adapt their production lines to include the process of printing or affixing the data carrier. In addition, they include scanners in their production lines to verify the validity of the codes.
  - They can print or affix additional data carriers in the aggregated packages to facilitate the tracking and tracing activities of wholesalers and distributors.

- **Wholesalers and distributors:**
  - They are in charge of the reporting of events of tobacco products along the distribution chain according to the TPD.
  - They have to adapt their scanning devices to be able to scan the data carriers included in the aggregated levels by their suppliers.
  - They can adapt their current scanning devices if their suppliers include additional data carriers.

- **Public authorities:**

Commented: I like this model........once they are approved, industry can choose.
They **have to** be equipped to be able to read the data carriers included in the unit packet and the aggregated levels.

As any previously approved data carriers is allowed, the scanning devices for Public Authorities will also only have to be able to scan numerous data carriers (or to have multiple devices to read all of them).
3.4. Allowed delays in reporting events

This section presents the options regarding the choice of the allowed delays in reporting events, which should ensure that the traceability and trade data are transmitted and recorded into the Tracking and Tracing Data Storage system, within the maximum allowed time lag, between the event occurrence and its effective report by the economic operator. As such, the allowed delay refers to the maximum time allowed to transmit the reports required by the TPD from the economic operator to the Data Storage system. The chosen option must be implemented in a cost-efficient manner meeting the defined primary and secondary requirements.

<table>
<thead>
<tr>
<th>EU Manufacturer / EU Importer</th>
<th>Transport</th>
<th>Distributor 1</th>
<th>Dist 2...</th>
<th>Consumer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1d</td>
<td>1d</td>
<td>1d</td>
<td>1d</td>
<td>1d</td>
</tr>
<tr>
<td>Uid</td>
<td>Aggregation</td>
<td>Expedition</td>
<td>Reception</td>
<td>Disaggregation</td>
</tr>
</tbody>
</table>

**Figure 28: A conceptual view of the possible event sequence generation in a timeline**

The image above depicts each economic operator, in a timeline, generating and reporting events to the Data Storage System.

The evaluation of distinct options of allowed delays is necessary because each delay will have different impact on the industry when performing the event reporting. However, data freshness should always be driven by the business requirements, not the technology itself\(^\text{36}\). Some economic operators may not actually support some of the given options of the Allowed Delays, as well as one option may work more efficiently to some economic operator than to others. For instance, among other situations:

- Facilities working in standalone (unconnected or with strong connection restrictions) would have an impact to implement an online event reporting.
- Facilities with connection restrictions would provoke several downtime periods jeopardizing the data transmit process.

---

Facilities working only with batch processing systems would have an impact to implement an online reporting.

The definition of the allowed delays for reporting events requires to differentiate the concept of frequency from the concept of delay:

- **Delay** is the time taken by the economic operator to report the Data Storage system with the event data since its occurrence, which is the actual subject of this section.
  
  Ex.: Considering a One Day Allowed Delay, if an event occurs at 10:00:00AM, the economic operator shall inform the system before 10:00:00AM of the following day.

- **Frequency** refers to the time in which data is fed at regular intervals. This often refers to whatever time/times (of the day, week, month, year, or in any given length of period) the data feed should happen. Frequency is not subject of this section.

Accordingly, with the TPD, two event data categories must be supported:

- **Traceability data** as previously defined in section 3.2;
- **Trade data** as previously defined in section 3.2.

The process of an event reporting must be accomplished within the maximum allowed delay, which includes: the whole process of data capture, any internal data processing needs and/or intermediary steps through the management systems (WMS, MES, ERP, UTrack), then finally the report of the event data to the Tracking and Tracing system. Taking that into account, it is envisaged that a too low allowed delay in reporting events may directly impact both, on the economic operator when regarding the necessary time to prepare and compile relevant data prior being reported, and on the Tracking and Tracing system when regarding the necessary time to validate, synchronize and process data prior being effective and ready to be used by the Competent Authorities.

The structure of the reported data should be based on public standards, such as **ISO/IEC 19987** previously explained on section 3.2, that shall contain the event’s occurrence timestamp, in a universal date time format such as UTC, in order to allow any further temporal event sorting, disregarding the event reporting sequence.

**Data exchanged: Connection rates and amount of data exchanged**

The total volume of transmitted data will not vary depending on the allowed delay, instead, the data volume variation will be per connection to report events to the Data Storage system. A near real-time system sends a smaller volume of data per connection while a one week delay sends a bigger volume of data per connection.

On a most demanding production activity scenario, an average of 2 events reported per unit packet is expected during the production process (UID generation and UID verification). The further movements (aggregation, dispatch, receipt, disaggregation, picking, re-aggregation etc.) produces up to 9 event reports per each group of 25,000 unit packets (a pallet), which represents only 0.018% of the total event reporting.
maximum size of an event report message is expected to be around 3KB, including all technical specs. Assuming such values, it is possible to calculate that for a production line speed of 1,000 packets per minute working 24x7x365, can generate in average, approximately up to 0.1MB of event data to be transmitted per second.

This rate leads to a conclusion that high connection rates are not required, instead, a standard market internet connection, such as ADSL, 3G can attend and support the expected throughput for all the given options.

Prevention of connection problems:

If a facility experiences any type of connection problem, the existence of a local data buffer area shall retain the event data until the re-establishment of the connection, then, the feeding process can recover from the buffer the sequence of events occurred during the eventual downtime. This buffer area is important in order to prevent data loss. To prevent the physical or technical connection issues it is foreseen that the defined system shall implement redundant connections to the Internet.

Surveillance and monitoring activities for Authorities:

For the analysis of the options all the limitations possibly encountered by the Competent Authorities during the realisation of audits and inspections, have also been considered, since the longer the allowed delay would represent a larger number of products inside the "blindness" period in the different Economic Operators, which means a range of time that is not possible to know either the existence of a new packet produced (period 1 of blindness) or the destination of the packet (period 2 of blindness). These two blindness periods are considered to be the greatest weakness of the surveillance process. (For instance, it has been also reported that EMCS functioning problems make the control by Competent Authorities very difficult).

Despite the allowed delay, before the movement of products to another facility, it is imperative for the transporter or receiver to have reported all the events that have occurred and the related data. Therefore, in case of an inspection, the Competent Authorities will then be aware of the events history, thus preventing sanctions which could include a potential product movement stoppage until the arrival of that respective information to the Tracking and Tracing system.

Impact on the local and central system processes and architecture:

Other aspects have also been considered for this analysis such as the direct impact on data storage areas, the local buffer and the Tracking and Tracing Data Storage, where the longer the allowed delay on reporting event is, the larger the required local buffer area will have to be in order to retain data prior being reported, and also the larger the Tracking and Tracing Data Storage Area will have to be in order to process data in order to ensure the completeness of the information.

Commented: My sense is that the 'sizing' of central storage is off balance and I have heard that all identifiers every assigned in this sector could fit on one USB key. More work on this is required.

Commented: ?????

Commented: the whole area of in-transit is critical and not covered. Including real-time tracking and tracing of the truck in transit and the ability to connect with the driver and click on a system to identify the contents of the truck. This needs to be covered...it's essential for control and surveillance and to mitigate the risk of in-transit theft.
Within this context, the Inception Impact Assessment\textsuperscript{38}, in its policy options, defined three alternatives to the allowed delays in reporting events. The right choice of the ideal option will depend upon business requirements and technical factors that will be evaluated in section 4.4 later in this document. The given options provoke distinct impacts over the solution, which depend upon when or how often the data must be analysed, as the event occurs or after the event occurs.

Option D1: Near Real-time Reports.

Option D2: One Day Delay Reports.

Option D3: One Week Delay Reports.

Each one of them will be explained on the following sections.

3.4.1. Near Real-time reports

In this option, the economic operator must commit to reporting event messages on a near real-time basis, meaning that a low-latency should exist between the event occurrence and the notification to the Data Storage system.

It is significant that near real-time data processing and analytics allow the ability to take immediate decisions when acting within seconds or minutes. That allows the Competent Authorities to obtain the information required to react prudently at the right time, which almost always means “immediately”.

It is important to clarify the difference between a hard real-time computer system from a near (soft) real-time computer system. The design of a hard real-time system, which always must produce the results at the correct instant, is fundamentally different from the design of a near real-time system. The demanding response time requirements of hard real-time applications, often in the order of milliseconds or less, must be highly autonomous to maintain safe the operation of the process.

Taken into the context of this Tracking and Tracing system, the implementation of a hard real-time would require that an event must be reported to the data storage within a millisecond following of its occurrence. This would thus demand that the whole economic operator's systems and process were prepared to perform all steps between the event occurrence and the event reporting within a matter of milliseconds. In contrast, a near real-time system can tolerate late answers. The response time requirements are often in the order of several seconds or minutes. That means, the event occurrence can be reported after a while, which will conclude to the total time lag between the actual event occurrence time plus the internal data movements time to confirm its occurrence. This is due to the existence of some economic operator's internal processes, for instance: An event occurs during a product expedition, this expedition must be confirmed by the expedition system, which must prior perform some calculations, and then it is sent to the ERP system to pass through an approval process that confirms the expedition. The latter, depends on the conclusion of several other expedition products and it takes up to 1 hour

Implementation analysis of a EU system for traceability and security features of tobacco products
Interim Report II

Consumers, Health, Agriculture and Food Executive Agency
Health Programme

74

In this case, all the processes between the actual time of the event occurrence and its reporting took some time and the event reporting will only materialize after that. In order to avoid the raise of several unreal suspicious movement alerts, a reasonable delay must be allowed to let the natural process occur prior being reported to the data storage system.

This allowed delay option refers to the near real-time computer system with the limit of up to a few minutes, for instance 60 minutes (1h), concluding to a continuity of event reporting concept. Considering allowing such a limit on reporting events, facilitates the economic operator to adapt to the event reporting process.

To illustrate the given concept above, considering a time interval of 2 weeks, starting from the day of the production of a unit packet, up to the moment of its delivery to the outlet retail, the first event would have happened on moment d1 and reported up to 1h after the moment d1, the dispatch on d13 and reported up to 1h after the moment d13, then the final delivery on the moment d14. This scenario leads to a maximum interval of about 13 days to have the full cycle of event data reported to the Data Storage, with 2 periods of blindness of less than 1 hour each, as shown on the image bellow.

The horizontal blue bar represents the possible occurrence of several other events before the last Dispatch event.

Having a 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 a low-latency. That means, any approve or confirmation of the event through management software, such as an ERP, and then, the event reporting, must be concluded within this allowed delay.

- A continual input and output of data process having data being processed in a small time period (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 to deal with faults or any unforeseen problems, such as connection downtimes.

A small amount of data sent several times, therefore reduces the volume of data to be sent per transmission, which means a very even and balanced volume of data transmission during a time frame.

The possibility for law enforcement to proactively analyse and react upon a potential risky event reported.

Once the pipeline of data constantly receives analytics in near real-time, as the operations take place, it completes the data feeding cycle and helps to analyse data as the event occurs.

3.4.2. One day delay reports

In this option, the economic operator must commit with reporting event messages within the maximum of one day after the occurrence of an event. That means every event must be delivered to the data storage before completing 24h of its occurrence.

A data feeding with maximum of one day delay, allows the prior data harmonisation and processing using a larger amount of time. Therefore, decisions are taken disregarding the exact second or minute of the event occurrence, which allows the Competent Authorities to obtain a daily processed and consolidated information.

Considering a time interval of 2 weeks, starting from the day of the production of unit packet, up to the moment of its delivery to the outlet retail, the first event would have happened on moment d1 and reported up to moment d2, the dispatch on d13 and reported up to moment d14, then the final delivery on the moment d14. This scenario leads to a maximum interval of about 13 days to have the full cycle of event data reported to the data storage, with two periods of blindness of 1 day each, as shown on the image bellow.
Figure 30: The timeline view of the events reporting and blindness periods of 1 day allowed delay

Having one day data reporting delay has the following implications:

- A large time lag tolerance on event reports, which allows the event data to be collected, processed by any internal economic operator’s system to approve or confirm the movement, such as an ERP, prior being sent to the Data Storage system.

- A lower fault-tolerant reporting system, on the manufacturers and economic operators side, in order to recover from data report process failure.

- The ability to handle, by the systems of manufacturers and economic operators, large amount of data without jeopardizing performance to process high volume of data accumulated within one-day time frame.

- One-day time lag on sending data, therefore, it increases the volume of data sent per transmission, when compared with near real-time reporting.

- Risk of sanctions or product transportation halts due to missing information on the Tracking and Tracing system.

- The possibility for law enforcement resources to analyse and react upon a potential risky event reported only within one day.

3.4.3. One Week delay reports

In this option, the economic operator will have to commit with reporting event messages within the maximum of one week after the occurrence of an event.

A data feeding with maximum of one-week delay, allows the prior data harmonisation and processing using a larger amount of time. Therefore, decisions are taken disregarding the exact second, minute or even the day of the event occurrence, which allows the Competent Authorities to obtain a weekly processed and consolidated information.

Note:
In a matter of clarification, considering a time interval of 2 weeks, starting from the day of the production of unit packet, up to the moment of its delivery to the outlet retail, the first event would have happened on moment $d_1$ and reported up to moment $d_7$, and the final delivery had happened on the moment $d_{14}$ and reported up to moment $d_{20}$. This scenario leads to a maximum interval of nearly 20 days to have the full cycle of event data reported to the data storage, with two large blind periods of 7 days each, as shown on the image below.

![Timeline Diagram](image-url)

**Figure 31:** The timeline view of the events reporting and blindness periods of 1 week allowed delay

Having one week maximum data reporting delay has the following implications:

- A very flexible and low fault-tolerant reporting system on the manufacturers’ and economic operators’ side.
- The ability by the systems of manufacturers and economic operators to handle very large amount of data collected during up to one week.
- Sending large amount of data up to after one week, therefore, it increases the volume of the data sent per transmission, when compared with one-day delay reporting.
- High risk of sanctions or product transportation halts due to missing information in the Tracking and Tracing system.
- The reporting time lag may seriously obstruct law enforcement actions.

**Commented:** You must track shipments, trucks etc. in any competent supply chain with highly regulated terms.

**Commented:** What does this mean specifically?
3.5. Method of adding a security feature

Article 16 of the TPD states the need of having security features on all unit packets of tobacco products placed on the market, as a medium 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 TPD also predicts the possibility to, whenever possible, combine what is required in Article 16 of the TPD with the security features currently implemented on the tax stamps or national identification marks used by Member States for tax purposes, provided that they fulfil all technical requirements. However, it is important to note that fiscal marks and security features are different topics, and even in Member States that do not apply any sort of fiscal marks, the requirements for security features set out in Article 16 of the TPD will still apply. To avoid further confusion, it is also important to note that the security features are not linked with the unique identifier or with any data carriers applied to tobacco products.

The definition presented here focuses only on how to add the security features to unit packets of tobacco products. The definition is therefore independent of any specific technologies (e.g. holograms, latent images, etc.) and to the levels of protection applied (i.e. overt, semi-covert, covert and forensic).

The Inception Impact Assessment, in its alternative policy options, defined three alternative methods to add a security feature:

**Option S1**: Affixing;

**Option S2**: Printing or integrating through a different method, and;

**Option S3**: Mixed solution (affixing and printing or integrating through a different method).

This provides for the possibility to combine several security elements, and adds an additional level of flexibility that can, ultimately, improve the integrity of the overall system. The figure below demonstrates how different security elements can be combined to generate a full TPD compliant security feature.
This combination of security elements can generate a stronger security feature, as for someone to engage in illicit trade of tobacco products it would be necessary to circumvent all security elements implemented.

The following sub-sections explain the specific implications of affixing, printing or integrating through a different method, or applying a mixed solution for the implementation of the security feature.

### 3.5.1. Affixing

The first option defined is affixing security features. This is the method of choice for Member States’ fiscal marks.

These affixed tax stamps or national identification marks also carry, in most cases, security elements of their own.

Affixed security features are considered as:

1. Impossible to copy: as the TPD predicts its implementation of both visible and invisible security elements, which are, by definition, impossible

   Even if an affixed security feature is photocopied and has the "look and feel" of the real security feature it should always be capable of being discovered upon control.

2. Secure the product they are applied to, according to what the TPD requirements to be tamper proof and irremovable: This can be attained using technologies such as frangible paper 39, which can be combined with security die cuts (or kiss cuts) to

39 In labelling, frangible paper is used to make thin, delicate materials for tamper evident labels. These materials have very little internal strength and structural integrity, meaning that if someone attempts to remove a label from a substrate, it will fragment into tiny pieces, which makes it extremely difficult to remove the label in its entirety and provides visual evidence that someone has attempted to tamper with it.

Commented: Governments have tried this for many years with paper money and many have failed, even with up to 5 security features. What can be referenced here to reflect on the challenge?

Commented: By whom? market surveillance, consumers? Economic operators? The benefits of a real-time system should be implied here.
To improve the integrity of this device, the affixed security feature should be placed in an area where the unit packets of tobacco products cannot be opened without breaking the feature.

Also, and whenever possible, the security features should be affixed before the unit packets of tobacco products get there cellophane wrapping, in order that the security features do not get destroyed during handling and transportation.

When considering all points considered above, affixed security features can be applied to all types of tobacco products, regardless of the size and typology of their unit packets.

3.5.2. Printing or integrating through a different method

The second option defined is printing or integrating a security feature through a different method onto unit packets of tobacco products.

This option guarantees, in principle, a better integrity of the system, as the security feature is directly applied onto the unit packets of tobacco products, which means it cannot be tampered with or removed without destroying the package. Apart from this, given the structure of the packs and the space available to apply them, this option can present more technological options.

Operationally, this option is a better fit for high speed / high production products – which in this context means cigarettes, which can be produced at more than 1000 packs per minute, and represent single-handedly the largest tobacco products’ market in the EU. It can also have reduced impacts on the manufacturers’ production process, as the security features can be printed or integrated through a different method directly on the production lines, or they can be printed or integrated through a different method at a previous stage (e.g. by their suppliers of packaging material). This option is viable for at least some security elements, and as long as if the security of the production environment, transportation, and storage, can be ensured.
For other types of tobacco products, and especially on smaller operations, this option may become harder to implement than an affixed security feature. This option may even become impossible to implement on very specific cases: cigars may come in wooden boxes, and products like cigarillos and pipe tobacco can come in metal tins, where the physical properties of the products makes it very hard to print security features (e.g. holograms) or integrate them through a different method (e.g. micro perforation).

![Figure 34: Wooden boxes and metal tins](image)

Given the difficulties presented, a certain degree of flexibility is recommended, in order to take into account the specifics of each production operation.

### 3.5.3. Any method

The third option defined enables the utilisation of both affixed and printed (or integrated through a different method) security features.

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

- The type of tobacco product: Printing or integrating security features through a different method can be more suitable for some types of tobacco products, while others may require those to be affixed. This choice should minimise the impact of the manufacturers’ operation, while complying with all requirements of Article 16 of the TPD.

- The Member State: Member States that already use tax stamps as a fiscal marking may adjust the security features already implemented in their fiscal markings to comply with the requirements of Article 16 of the TPD. This option should always be implemented with the interests of all stakeholders in mind, both public and private.

It is necessary to add, however, that regardless of the option chosen, the TPD does not forbid any manufacturer to implement other security elements that they may consider necessary for the security of their operation.
4. Evaluation of the Alternative Policy Options

The options initially proposed by the Commission in June 2016 were used for the Public Consultation open from the 29th July to the 4th November 2016. The first step of our approach is the refinement of the options proposed in the Inception Impact Assessment.

Following the main options under evaluation are as presented below.

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

Table 7: Refined alternative policy options, based on the Inception Impact Assessment

The alternative policy options are firstly evaluated against a set of selection criteria predefined by the Commission. These criteria, and our understanding of each one of them, is presented below:

- Full compliance with Articles 15 and 16 of the TPD and Article 8 of the FCTC Protocol: The option complies with all the requirements established in Articles 15 and 16 of the TPD and Article 8 of the FCTC protocol;
- Technical feasibility: The option is technically feasible and can be implemented throughout the economic operators and public authorities;
- Interoperability (with key users’ and other company’s systems): The option guarantees the interoperability with the systems of key users (both national and international).
European authorities), and with the systems of the economic operators (e.g. to access information that needs to be included in the data carriers);

- Ease of operation: Once it is implemented, the option is easy to operate by the various stakeholders;
- System integrity: The option performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation of the system;
- System security: The option ensures or implements proper controls of the accesses to all system resources and data;
- Potential of reducing illicit trade: The degree in which the option contributes to the reduction of illicit trade;
- Burden for economic stakeholders: The financial/ economic impact for the economic operators generated by the option;
- Burden for public authorities: The financial/ economic impact for the public authorities generated by the option.

These selection criteria apply to all alternative policy options, which enable a standard comparison and, ultimately, the selection of the optimal high level solution. To identify the optimal option, however, the selection criteria are added up, with different weights, until a final score by option.

Based on the results of the high-level impact assessment, four main groups of impacts emerge and with it define the weightings for the secondary requirements (or selection criteria):

**Figure 35: Weighting of the selection criteria**

The scoring of the evaluation criteria is the basis of the whole scoring process. For the purpose of this evaluation, an "eight piece" scoring model was defined, which translates...
Implementation analysis of a EU system for traceability and security features of tobacco products
Interim Report II

into having each option being rated as 0 – 12.5 – 25 – 37.5 – 50 – 62.5 – 75 – 87.5 – 100% in their performance in each evaluation criteria.

In the specific case of the primary (or mandatory) requirements, the only applicable scoring options were 0 and 100%, meaning that the option either complies with the mandatory requirements, or does not, being cast out of the evaluation. For the secondary (or optimization) requirements, the full spectrum from 0 through 100% applies.

The scoring of each option in the evaluation criteria defined is accompanied by a detailed justification, which allows the understanding of how each option ranks compared to its peers. This can be found on chapter 7. ANNEX A: DETAILED EVALUATION OF EACH POLICY OPTION.

4.1. Governance model
4.1.1. Primary requirements
4.1.1.1. Full compliance with TPD and FCTC Protocol

The primary requirement of the optimal system is its full compliance with articles 15 and 16 of the TPD and article 8 of the FCTC Protocol.

On the basis of the legal analysis carried out by the team, it can be concluded that all the three alternatives may meet the primary requirements. However alternative A1 – industry operated solution will only be compatible with the legal requirements as-long as extensive additional control measures are put in place (see Chapter 3.1.1.). Without such extensive additional control measures, the industry will be the main entity controlling its own activity, which will represent a conflict of interests, potentially undermining the fulfilment of the TPD main objectives, i.e. establishing a Tracking and Tracing system which is required to be independent and transparent. In this context, due regard should also be given to the Protocol, which requires the Tracking and Tracing system to be controlled by the Parties.

For alternative A2 – third party operated solution, independence of the third party is a key guarantee for Member States that there is no conflict of interest vis-à-vis the industry.

In alternative A3 – mixed solution, independence of the third party (or the state agency) is a key guarantee for Member States that there is no conflict of interest vis-à-vis the industry. This is provided through a third party or a state agency which would be responsible for parts of the system which are deemed essential for exercising the overall control of the system (e.g. generation of the unique identifier).

Commented: It’s not a conflict of interest to management your own business. I think what you mean here is a conflict with the protocol. Suggest to rephrase

Commented: Another option here is where the code is generated by the industry but the encryption key is generated by the 3rd party of government agency. This is a viable option that should be considered.
4.1.2. Secondary requirements

4.1.2.1. Technical feasibility

Alternative A1 (industry operated solution) scores the highest in the technical feasibility. Being the industry in charge of managing the system (under close supervision and control of the competent authorities during the processes of generation of the unique identifiers and the printing or affixing, in order to ensure that all the unit packs of tobacco products are marked and that the unique identifiers are, indeed, unique), this is the alternative with less impact on the production processes.

Alternative A3 (mixed solution) presents as well a high score in terms of technical feasibility. All the operational processes are still performed by the industry, while the generation of the UIDs is allocated to an independent third party or a competent authority. The ability to transmit this UID to the industry so that it can be consolidated in the data carrier with other relevant information and printed or affixed in the packet without delays is the main challenge of this alternative regarding the technical feasibility.

Alternative A2 (third party operated solution) presents on the contrary the weakest score in terms of technical feasibility. This alternative implies the presence of equipment and personnel in the facilities of the industry, to install, operate and maintain the T&T system. The potential negative impact on the production process is high compared with the other two alternatives.

4.1.2.2. Interoperability (with key users’ and other company’s systems)

Alternative A1 (industry operated solution) presents the highest in the technical feasibility. Being the industry in charge of managing the system (under close supervision and control of the competent authorities during the processes of generation of the unique identifiers and the printing or affixing, in order to ensure that all the unit packs of tobacco products are marked and that the unique identifiers are, indeed, unique), this is the alternative with less impact on the production processes.

Alternative A3 (mixed solution) presents as well a high score in terms of technical feasibility. All the operational processes are still performed by the industry, while the generation of the UIDs is allocated to an independent third party or a competent authority. The ability to transmit this UID to the industry so that it can be consolidated in the data carrier with other relevant information and printed or affixed in the packet without delays is the main challenge of this alternative regarding the technical feasibility.

Alternative A2 (third party operated solution) presents on the contrary the weakest score in terms of technical feasibility. This alternative implies the presence of equipment and personnel in the facilities of the industry, to install, operate and maintain the T&T system. The potential negative impact on the production process is high compared with the other two alternatives.
Several sources point to the importance of the use of open standards to contribute to the global effectiveness of a T&T.

Alternative A1 scores low in this criterion, as the proprietary nature of the systems developed by the industry challenge the whole interoperability of the system. The whole configuration of alternative A1 is based on the systems developed and operated by the industry itself. The interoperability of these solutions with the systems of other companies involved in the supply chain of tobacco products is at stake.

In the contrary, in alternative A2 (operated by independent third parties), the interoperability is enhanced as they shall work based on technical standards. Alternative A3 would be in an intermediate position, as the generation of the UIDs is meant to be done by an independent third party and/or the competent authorities, while industry would be in charge of overseeing marking each unit of tobacco products and scanning and verifying the codes.

**4.1.2.3. Ease of operation**

The configurations detailed in alternatives A1 and A3 score the maximum in the criteria of ease of operation of the system. In both alternatives, the industry is in charge of overseeing the operational processes (printing or affixing and scanning/verifying the codes) and public authorities and third parties’ involvement is limited to a certain level of control. These two alternatives score higher in ease of operation compared with alternative A2. In the alternative operated by independent third party, however, the ease of operation of the system is jeopardised, as it requires permanent presence of personnel of the independent third parties in the facilities of the manufacturers to install, operate and maintain their equipment.
There are always risks on the generation of the unique identifiers, whether this is performed by the industry or by a third party, but these risks are the same across the three alternatives. However, there are several controls that can be implemented and that can be relevant, such as:

- Generation should take place in a secure, controlled environment with appropriate security measures in place to protect the central server, and only authorised parties should be allowed to request for codes.
- Across all the alternatives, audits performed by external auditors and by the competent authorities are foreseen; to increase the security of the generation of the UIDs.
- The algorithms used to generate the serialized identification codes and the methods of key encryption should be securely protected and kept secret for unauthorised parties as per business confidentiality and privacy rules and guidelines.

4.1.2.6. Potential of reducing illicit trade

There is always potential to reduce illicit trade. This is the main goal of the implementation of the tracking and tracing system. This is the goal as well of the TPD. The three alternatives presented in this Interim Report II for a governance model are not in contradiction with the obligations set in the Directive, as explained above. They are aligned with the aim of the system and may be regarded as reasonable governance models to achieve the objectives of the TPD. Therefore, we cannot favour any of the three alternatives when evaluating their potential to reduce the illicit trade. If we had considered that one of the alternatives contribute less to the reduction of illicit trade, we would not have concluded that the three of them are not in contradiction with the obligations of the TPD.
When analysing the burden for public authorities, there is an important difference between alternative A1 (industry operated solution) and the other two alternatives. As discussed when analysing the legal compliance of the three options, we have concluded that the TPD does not explicitly forbid the industry to be in charge of generating the UID and printing and affixing them into all units of tobacco products. However, the TPD requires that the Member States ensure that all unit packets of tobacco products are marked. In addition, any solution must fulfill the requirement of independency and control as set out in the section on legal assessment. Therefore, in alternative A1 the competent authorities must put in place very intensive controls over the whole system, to meet the requirements of the TPD. These intensive controls are translated in higher costs. An analysis of the allocation of these costs will be included shortly.

For alternatives A2 and A3, the financial burden for the public authorities presents minor differences.

4.1.3. Conclusion - Selected alternative

When considering all selection criteria, and the weighting defined, the final results point to option '(A3) Mixed Solution’ as the best alternative for the governance model.

The selected option allows a split of responsibilities between actors (manufacturers/importers, third party solution provider and public authorities) in order to ensure maximum control, integrity, transparency and independency of the system, while guaranteeing high technical feasibility and causing minimum disruptions in the production lines of the manufacturers and facilities of the importers.

From an economic point of view, it is also the alternative with lowest global costs, as seen in detail in the cost analysis.

The results of the scoring of the secondary requirements are depicted below:
4.2. Data storage models

4.2.1. Primary requirements

4.2.1.1. Full compliance with TPD and FCTC Protocol

Regarding legal compliance, all four options defined guarantee a full compliance with Articles 15 and 16 of the TPD and the FCTC Protocol.

The four alternatives are compatible with the legal requirements:

- All the options \textit{are able to} store the entry, intermediate movements, the final exit of the unit packets of tobacco products, the aggregated packaging information, and the trade information.

- All the options allow for recording, consolidating and making available all relevant data to the Competent Authorities and the Commission.

- All the options provide mechanisms to guarantee the establishment of access control policies \textit{according to} the TPD and FCTC.

- All the options guarantee that the tobacco industry will not be able to perform any obligations assigned to the Competent Authorities.

This fulfilment will be mostly accomplished through the usage of open standards such as ISO/IEC 19987:2015 EPC Information services, which provides specifications of many of the capabilities required by the Tracking and Tracing system. Therefore, if the options are based on this standard, or another with the same features, this criterion could be considered fully accomplished.

4.2.2. Secondary requirements

4.2.2.1. Technical feasibility

Option B1, centralised model, is the most feasible option with regards technical feasibility. This is due to several factors: a) has better efficiency for reading and writing accesses because the underlying architecture is simpler than the distributed models, and b) up-to-date technology is available and real production references of such scale are known.

Notwithstanding, the centralised model poses a major challenge to be addressed regarding the issue of enabling a single point of cyber-attack meaning that, in case of disruption of this central service, the update of information by the industry and all the economic operators within the supply chain would be untracked and untraceable.

Moreover, irrespective of the option, it should be remarked that the Tracking and Tracing system also has a data sizing challenge. Therefore, it is highly recommended to embrace data storage best practices for large scale systems such as the following\(^\text{41}\): establish separate physical data storage areas according to the project needs and priorities such as frequency of access (e.g. the more often accessed should be stored in the quicker storage tier), age of data, protection or specific business rules. Thus, such tiered storage environment can deliver the required combinations of performance, capacity and resilience.

As a minimum, two tiers of data are recommended according to current state of play\(^\text{42}\): “hot” tier with low response times and “cold” tier with higher response times.

Options B2 and B3, with decentralised models, have the lowest scoring because of the following drawbacks: a) their architecture adds additional complexity to the overall solution (in comparison with the centralised) because it means the need of additional components (e.g. Discovery Service, etc.) that would introduce additional delays, other potential points of failure, more development and maintenance costs, etc.; and b) introduces a penalty on

---


\(^{42}\) Amazon webservces (AWS) - Storage and Database best practices - http://www.slideshare.net/AmazonWebservices/dat203-28463220
the read/write performance; and c) there are no up-to-date technology nor reference systems that realize such federated capabilities.

Hence, with regards the technical feasibility, the conclusion is that Option **B1 comprises globally the best characteristics**, namely: a) efficient read/write data access, and b) availability of up-to-date technology, and standards, that support the solution.

**Finally**, it should be noted, that irrespective of the option, the Track and Trace system has a data sizing challenge ahead. Therefore, it is highly recommended to embrace data storage best practices for large scale systems such as the following:\footnote{European Commiss on: 2016 Best Practice Guidelines for the EU Code of Conduct on Data Centre Energy Efficiency - http://iee.jrc.ec.europa.eu/energyefficiency/strategies/energyefficiency/files/files/CDC_DC/2016/2016_best_practice_guidelines_v7.1.2.pdf} establish separate physical data storage areas according to the project needs and priorities such as frequency of access (e.g. the more often accessed should be stored in the quicker storage tier), age of data, protection or specific business rules. Thus, such tiered storage environment can deliver the required combinations of performance, capacity and resilience.

As a minimum, two tiers of data are recommended according to current state of play\footnote{Amazon web services (AWS) - Storage and Database best practices - http://www.slideshare.net/AmazonWebServices/datas203-28463220}: “hot” tier with low response times and “cold” tier with higher response times. When required, data could be moved between tiers automatically.

4.2.2.2. Interoperability (with key users’ and other company’s systems)

![Figure 49: Data storage model – Interoperability (with key users’ and other company’s system)](image)

**Interoperability with key users**

All four options guarantee full interoperability with the systems of the key users. Regardless of which option is chosen, the relationship between the national authorities and OLAF – JRC and CHAFEA should be guaranteed.

The interoperability is guaranteed through the services published by the Consumer Interfaces layer, which will support any additional extension, based on open standards. All
Implementation analysis of a EU system for traceability and security features of tobacco products
Interim Report II

four options publish the Consumer Interfaces layer that facilitates the integration with external systems and provides full access to the Competent Authorities.

**Interoperability with other companies’ systems**

Concerning the interoperability with the systems of manufacturers and importers, none of the options identified any causes specific interoperability issues to interoperate with them. All the options publish the same interfaces to these stakeholders.

However, concerning the interoperability with the distributors and wholesalers, it should be remarked their current IT maturity level is not as high as the manufacturers and importers. As such, the Study considers that the time needed to establish the integration of such systems with the new Track and Trace system might be longer than for manufacturers/importers.

Hence, all options score the same with regards interoperability.

**4.2.2.3. Ease of operation**

![Chart showing data storage model ease of operation](chart)

**Option B1**, centralised model, has the best scoring because, in comparison with the other options, introduces the minimum impact since there is no intermediate component when reporting the required data to the Data Storage system. Also, considering all the systems as whole, operate a single storage facility is less complex than several facilities, even if dealing with a big volume of data.

Option B4, combined model, has the second scoring. It is lower than B1 because this model is considered a bit more complex to operate since it comprises several facilities. Also, the additional delay caused to the wholesalers and distributors that use the Repository Router is considered an operational drawback.

Hence, with regards the ease of operation, the conclusion is that Option B1 comprises globally the best characteristics, namely: a) minimum impact on all the economic operators because no intermediate system is needed (i.e. all the economic operators report directly to the central Data Storage system), and b) “easy” operation because there is only one storage facility to maintain.
4.2.2.4. System integrity

Option B1, centralised model, has the best scoring because it provides the best balance with regards physical integrity (i.e. complete assurance that under all conditions a system maintains correctness, completeness and reliability of its major assets: hardware, software and data) and data integrity (i.e. degree of minimising data inconsistencies).

The former is achieved because actually B1 comprises less sub-systems that would rather simplify the protection and fault tolerance (in comparison with the other models) of its components. The latter is granted by the data consistency checks conducted at the central Data Storage system. If the data is centralised, its integrity is better reinforced.

Options B2 and B3, decentralised models, score lower because in distributed systems: a) the physical integrity is more difficult to achieve, and b) data integrity is also more difficult to assure.

Hence, with regards the system integrity, the conclusion is that Option B1 comprises globally the best characteristics, namely: a) physical integrity, and b) data integrity.

4.2.2.5. System security

Within this category, all options score the same with regards system security.
The two criteria assessed: secure storage (i.e. minimise risk of potential security threats) and b) guarantee of control the access to data, score different per option depending on its underlying architecture.

As per centralised models, the access control to data can be enforced more easily than with a distributed architecture. However, the centralised model poses the big challenge of being a single point of access that could be attacked.

Hence, with regards the system security, the conclusion is that all the options have a good and equal scoring, but posing different drawbacks depending on the option.

### 4.2.6. Potential of reducing illicit trade

![Data storage model – Potential of reducing illicit trade](image)

This criterion is driven by the degree of effectiveness on accessing all relevant data by the Competent Authorities in order to retrieve the information needed to conduct surveillance activities. The higher effectiveness on read accesses, the higher potential ability to reduce illicit trade.

As such, B1 and B4, with centralised data repositories, are the ones that best helps accomplishing the criterion of potential of reducing illicit trade.

### 4.2.7. Burden for economic stakeholders

![Data storage model – Burden for economic stakeholders](image)
**Option B1**, centralised model, has the best scoring because its costs are the lowest. This is due to the fact that because this option comprises solely of a single system. Although it requires demanding hardware infrastructure to host and manage the expected sizing of the whole Tracking and Tracing system, in comparison with the costs of the other models is much lower. Details of the cost estimations, the assumptions and what is included can be checked in Annex 8.2 Data storage -storage.

Options B2 and B4, decentralised as per manufacturer/importer and combined, are expected to have a similar number of systems. As such, their cost is similar, but higher than B1. The cost of B3 is higher than B2 and B4 because it has been assumed that at least 15 Member States would wish to have their own database, based on the consumption per country.

Finally, it should be remarked that the costs are an estimation, based on objective assumptions. However, many things are still pending to be decided and the costs may vary and could not be considered as definitive.

### 4.2.2.8. Burden for public authorities

![Figure 55: Data storage model – Burden for public authorities](image)

This criterion is driven by the labour costs of the public authorities concerning the activities to be conducted with regards the supervision of contracts that have must be concluded with the independent data storage service provider. Also, the supervision of the auditing activities has been considered. Details of the cost calculation can be checked in Annex 8.2 Data storage -storage.

As such, Option B1, centralised model, requires the lowest administrative efforts because there is one single system to approve, monitor and evaluate the third-party data storage provider contract.
4.2.3. Conclusion - Selected alternative

The final results of the assessment point to option ‘(B1) Centralised model’ as the best alternative for the data storage model.

Along the evaluation, it has been assessed that the selected option, B1, scores the best (or at least equal) than the other options. This helps ensuring a high level on reliability when appointing for this option because performs well in all the categories assessed. On top of this, there are real references of systems with central repositories (e.g. EU Schengen Information system, TRACES - TRAdie Control and Expert System and China’s system for tracing pharmaceutical products).

When analysing all the selection criteria, it is important to note that all options defined secured a perfect score on the primary requirements defined by Chafea. The results of the scoring of the secondary requirements are depicted below:
4.3. Allowed data carriers

4.3.1. Primary requirements

4.3.1.1. Full compliance with TPD and FCTC Protocol

One of the primary requirements of the optimal system is its full compliance with articles 15 and 16 of the TPD and article 8 of the FCTC Protocol.

The five alternatives are compatible with the legal requirements:

- They are able to contain the unique identifier and all the information specified in the article 15 of the TPD at the unit packet level.
- They are able to embed the identification at the different aggregation packaging levels.

4.3.2. Secondary requirements

4.3.2.1. Technical feasibility
All the options present similar scoring in terms of their technical feasibility, however option C2 is the alternative with highest score.

Options C3, C4 and C5 obtain a better adaptability score in evaluation parameters such as:
- Ability to adapt the data carrier to the unit packet of tobacco product
- Impact generated by the printing or affixing activities on the manufacturer and importer production processes

Nevertheless, the options C1 and C2 present a better adaptability to other evaluation parameters:
- Availability of different suppliers
- Ability to adapt to quality control activities

In terms of feasibility with wholesalers and distributors, the alternatives that enable optional addition of data carriers (C2, C4), present better adaptability than the rest.

### 4.3.2.2. Interoperability (with key users’ and other company’s system)

The number of allowed data carriers has an effect on the capacity of the stakeholders to read them. A reduced set of data carriers improves the compatibility with the operational equipment. The possibility of optional data carriers enables the integration with the economic operators of the distribution chain.

It can be stated that:
- The interoperability with manufacturers’ and importers’ systems is similar for all the options.
Implementation analysis of a EU system for traceability and security features of tobacco products
Interim Report II

- The interoperability between trading parties is significant impeded when proprietary unique identifiers are part of the system; whether provider by governments of 3rd parties.
- Proprietary unique identifiers are non-interoperable and can only successfully exist within a monopolistic and proprietary system.
- The interoperability with key users, wholesalers and distributors' systems is reduced when the number of data carriers increases.

4.3.2.3. Ease of operation

![Diagram showing data carriers for each option]

With regards to the ease of operation criteria, all the options obtained a similar score, where options C1, C2, C3 and C4 scored slightly higher.

The impact on the operational processes of the manufacturers and importers is similar for all of them, due to the fact that it depends on the selected data carrier.

However, the impact on the wholesalers' and distributors' operations is lowest in the options C1 and C2, followed by option C4.

Due to the number of allowed data carriers, the options C3, C4 and C5 have less impact on:

- Printing and affixing performance
- Scanning speed and reliability
4.3.2.4. System integrity

The system performance and the system reliability are less affected with the application of a reduced set of allowed data carriers. Therefore, the integrity of the system is not challenged when the system interacts with a single data carrier (alternatives C1, C2).

There is limited risk of integrity breaches in C3 and C4, as the number of allowed data carriers is increased. The risk escalates when the option of a free system is considered. Such a system enables any allowed data carrier, which can in turn impact the system performance, system reliability and result in unexpected functioning.

4.3.2.5. System security

In terms of system security, options C1 and C2 obtain the best scores. These envision that a lower number of allowed data carriers provide a more secured environment,
associated with a reduction in unauthorised manipulation, tampering or falsification of the selected data carriers. When the number of allowed data carriers increases the environment’s security is more challenged.

The risk for the security of the system is not inherent to the number of data carriers itself, but also to the type of data carriers used, as each particular type implies a different level of security. However, while the risk is not inherent to the number of data carriers, it must be further emphasised that an increase in the different types of data carriers used will result in an increase of the probability of having a non-secure one between them. Therefore, an increase in carrier types will also require an increase in control over the selection of data carriers for the system, in turn making this factor a risk for the system’s security.

4.3.2.6. Potential of reducing illicit trade

The allowed data carriers have a direct proportionality with the potential of reducing the illicit trade. A system that permits the use of a single data carrier (C1, C2) is more efficient and strong. This enables the easier identification of potential irregularities, limiting the risk.

A system that contains a limited number of data carriers is easier to control by the public authorities, creating a more secure and efficient environment. So, as the number of data carriers is increased, the potential of reducing illicit trade is reduced.

Nevertheless, as it was stated in the previous section, the potential of reducing the illicit trade is not inherent to the number of data carriers itself but to the type of data carriers used. However, an increase in the number of allowed data carriers is more probable to challenge the objective of reducing illicit trade.

Commented: This is complete nonsense.

Commented: This is an unqualified assumption without facts. This whole section is very weak and shows a poor understanding of data carriers and the linkage to security, interoperability and trade.

Commented: As above, incorrect and inconsistent with previous and following paragraph.

Commented: See above.
4.3.2.7. Burden for economic stakeholders

Regarding the burden for economic stakeholders, the options C1 and C2 are scored the highest because they represent the lower cost. However, they did not get a 100% because an economic effort is necessary to implement those options.

The burden is different depending on the type of economic operator:

- The cost for manufacturers and importers is similar because it depends on the selected data carrier instead of the total number.
- The cost for wholesalers and distributors is lower in options C1, C2 and C4 because they need to adapt their equipment to either one data carrier or to the optional data carriers if their suppliers added them to the aggregated levels.

Additionally, the process of adding new allowed data carriers to the free system may present some difficulties in the process of adaptation to manufacturing operations, which will incur extra costs.
4.3.2.8. Burden for public authorities

In terms of burden for public authorities, the options C1 and C2 are scored the highest because they incur the lower cost. Although it is considered the economic effort represented.

The economic impact of the allowed data carriers on the public authorities is minimum when a single data carrier is considered because the cost associated to the system and to the equipment is lower for those alternatives.

As the number of allowed data carriers is increased, the cost of the equipment necessary to audit and inspect is elevated. In addition, the process of including new allowed data carriers to the free system will introduce extra costs.

4.3.3. Conclusion - Selected alternative

When considering all selection criteria, and the weighting defined, the final results point to option "(C2), a system with a single data carrier per identification level and optional data carriers for aggregation packaging levels" as the best alternative for the allowed data carriers.

Commented: Incorrect unless evidence is forthcoming. I have personally worked with different EU commissions, market surveillance, WCO, OECD and others to help them understand how to use the single GS1 system today where any standards based data carriers can be checked for ownership.

Commented: Partially true. That’s not the ‘real issue’. A data matrix is currently not used in distribution because it’s not required…simple as that. We need to have a verbal debrief on these points.
As noted earlier, the methodology and software needs to be exposed.
4.4. Allowed delays in reporting events

This section presents the evaluation of the criteria for the decision point regarding the “Allowed delays in reporting events”.

4.4.1. Primary requirements

4.4.1.1. Full compliance with TPD and FCTC Protocol

All three options defined can guarantee a full compliance with Articles 15 and 16 of the TPD and the FCTC Protocol:

Ability of transmitting data of the entry, intermediate movements and the final exit of the unit packets of tobacco products: The solution should be based on open and mature standards, such as ISO/IEC 19987:2015 EPC Information Services. This standard specifies an abstract supply chain data model, which informs about the different events that may happen, and how can be exchanged to be stored later.

Based on this standard, the GS1 System Architecture envisages different message formats, which fit with the allowed delay options.

Finally, it should be noted that many studies recommend the usage of ISO/IEC 19987:2015 EPC Information services (formerly named GS1 EPCIS) on the basis of its completeness, flexibility and proved functioning in international supply chain production systems.


46 GS1 System Architecture Document -
http://www.gs1.org/sites/default/files/docs/architecture/GS1_System_Architecture.pdf

47 FCTC - Analysis of the available technology for unique markings in view of the global track-and-trace regime proposed in the negotiating text for a protocol to eliminate illicit trade in tobacco products -

48 Rx-360 Traceability Data Exchange and Architecture Workgroup - White Paper on Traceability Data Exchange Architecture -
Therefore, if the options are based on this standard or another with the same features, this criterion could be considered fully accomplished.

**Ability of transmitting data of any transaction of tobacco products:** In addition to the above, this standard also specifies how to exchange trade information to be stored later. As such, this criterion could be considered fully accomplished.

### 4.4.2. Secondary requirements

#### 4.4.2.1. Technical feasibility

![Figure 70: Allowed delays in reporting events – Technical feasibility](http://www.diva-portal.org/smash/get/diva2:24156/FULLTEXT01.pdf)

The three alternatives are technically feasible; however, they differentiate on the following aspects:

**Overall Implementation Complexity:** The computational complexity of algorithms constructing a data delivery tasks, takes into consideration several aspects, i.e., the number of CPUs, type of conditions and deadline. Option D1 demands a medium degree of system complexity in order to ensure that the whole value chain is properly adequate with the requirements of such option, including the complexity of gathering and compiling data in a shorter time, prior the reporting. Nevertheless, considering the actual technological scenario and the given period of adaptation, this complexity can be considerably mitigated, although, the other two options conclude to a low degree of complexity and are closer to the majority actual reality applied on the economic operators' data reporting, accordingly with the result of the Stakeholders Management of Real-Time Data Consistency and Transient Overloads in Embedded Systems - [http://www.diva-portal.org/smash/get/diva2:24156/FULLTEXT01.pdf](http://www.diva-portal.org/smash/get/diva2:24156/FULLTEXT01.pdf)
Consultation Survey\textsuperscript{50} and with the Public Consultation\textsuperscript{51}, both performed during the Feasibility Study\textsuperscript{52}. It is important to notice that on Option D1, when a too low delay is allowed, it increases the complexity not only on the economic operator when regarding the necessary time to gather and compile the data prior being reported, but also on the Tracking and Tracing system when regarding the necessary time to validate, synchronize and process the data prior being effective and ready to be used by the Competent Authorities.

**Complexity on managing the volume of data on the Local Buffer**: Prior to being reported to the Tracking and Tracing system, the data is retained in a local buffer area, first of all used to decouple the production process from the data reporting process, and secondly to keep the data stored prior being reported. The buffer area needs can highly increase depending on the period of the retention. Therefore, the complexity of handling a lower volume of data imposed by option 1, which can be very small and less demanding, scores to low level of complexity, whereas the other options, as the data retention time increases, the operation complexity also increases, reflected on the growth of the volume of data to be processed and transmitted in a more concentrated period of time, which leads option 2 to a high level of complexity and option 3 to a very high level of complexity. For instance, when having one week time lag, the volume of data captured during this interval can be thousand times bigger than when reporting on option D1, therefore, the volume of the retained data highly increases for option D3.

4.4.2.2. Interoperability (with key user’s and other company’s systems)

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure71.png}
\caption{Allowed delays in reporting events – Interoperability (with key user’s and other company’s systems)}
\end{figure}

\textsuperscript{50} Targeted stakeholder consultation on the implementation of an EU system for traceability and security features pursuant to Articles 15 and 16 of the Tobacco Products Directive 2014/40/EU - \url{http://ec.europa.eu/health/tobacco/consultations/2015_tpd_consultation_en.htm}

\textsuperscript{51} Public consultation on the implementation of an EU system for traceability and security features pursuant to Articles 15 and 16 of the Tobacco Products Directive 2014/40/EU - \url{http://ec.europa.eu/health/tobacco/consultations/2016_traceability_security_features_en.htm}

\textsuperscript{52} Feasibility study regarding the establishment of an EU system for tracking and tracing of tobacco products and for security features - \url{http://ec.europa.eu/health/tobacco/docs/2015_tpd_tracking_tracing_frep_en.pdf}
Interoperability is a characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, present or future, in either implementation or access, without any restrictions.\footnote{Interoperability Working Group - Definition of Interoperability - \url{http://interoperability-definition.info/en/}}

**Interoperability with key user’s systems:** All three options offer full interoperability with the systems of the key users. Regardless of which option is chosen, the relationship between the national authorities and OLAF – JRC and CHAFEA should be guaranteed.

This decision point “Allowed Delays in reporting events” regards the data reporting to the Tracking and Tracing Data Storage System. Despite that, it can be foreseen the next step, when a key user’s system may require to integrate with the Tracking and Tracing system, then at this point, the allowed delay may impact on the interoperability if the key user’s system requires a high level of data freshness, as envisaged on the EMCS - Functional Excise System Specifications of the Taxation and Customs Union (TAXUD)\footnote{Functional Excise System Specifications – TAXUD - \url{http://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/taxation/excise_duties/circulation_control/emcs_info_services/fess_leaflet_en.pdf}}, only possible to be accomplished by the near real-time, therefore option D1, due to its broader level of data freshness achievement, in a preliminary approach, is closer to be the optimal solution, at the same time, option D1 can also attend the requirements of any system with lower level of data freshness needs.

**Impact on the economic operator’s information systems:** All three options offer full interoperability with other company systems, and that applies to the need of having to be integrated with the company’s systems. Option D1 demands the economic operator’s system to become fully able to interact with the near real-time data requirements, which may conclude to increase the complexity to interoperate with already existing systems running on a lower level of data freshness rate, therefore, this option implies a medium impact on the economic operator’s information system.

Options D2 and D3 due to their longer time lag, are more capable to interoperate with the actual economic operator’s information systems, implying a lower impact then option D1, although a substantial impact is not discarded.

**Ability to interoperable with any other supply chain equipment:** Option D1 demands the supply chain equipment to be fully able to interact with the near real-time data requirements, which may conclude to a medium impact on the supply chain equipment.

Options D2 and D3 due to their longer time lag, are more capable to interoperate with the actual manufacturers’ equipment, implying both on a low impact on the supply chain equipment.

\footnote{Interoperability Working Group - Definition of Interoperability - \url{http://interoperability-definition.info/en/}}

This decision point ensures that a system is prepared to be able to detect incomplete transactions, and undo the portion of any incomplete transactions that are found. Nevertheless, system integrity also refers to the trustworthiness of the data resources. If data are missing important relationship linkages and are unable to link correlated records together, then they may lead to doubt on its reliability. System integrity brings the assurance that the data can be integrally accessed by those authorized. Besides, it is one important criteria of ensuring data quality.

The options present three distinct behaviours on system integrity:

**Information Consistency**: On option D1, on low limited delay process, an eventual system breakdown, communication instabilities or any other procedural point of failure, may lead to a data consistency fault that will demand a process of data validation or data recovery such as a data error detection feature. Options D2 and D3 are not so susceptible to such point of failure, as they allow the economic operator’s system to have a larger time to deliver report events, the data integrity verification can be performed in a more extend time, therefore, any data inconsistency can be checked and adjusted within the allowed delay.

**Information Completeness**: Option D2 and mostly option D3 poses a problem on the Tracking and Tracing system when regarding to detect the completeness of the events reporting cycle. A longer time lag delay allows data to be reported out of sequence, therefore, some earlier occurred event data can be reported up to one week after, while other later occurrences can be reported before, thus, the data integrity will be highly impacted until the completeness of the reporting cycle.

**Information Readiness and Information Effectiveness**: Option D1 is the most persistent, having a higher data transmitting rate, which leads to an optimal degree of data readiness and data effectiveness which increases the score for this option. The option D2 has a medium level of persistence leading to a lower level of data readiness and data effectiveness which concludes to a less effective approach, therefore receiving a medium score. At last, the option D3 has a very a large period of time between the event occurrence and its report, which leads to a score of low degree of data effectiveness and data readiness. This excessive large time between the event occurrence and its reporting leads to a severe lack of data readiness.

However, to fulfil integrity, data must undergo many controls. Thus, additional time is needed to control and validate data. In such circumstances, information may be not

---


available in the destination in timely fashion, thus the near real-time requirement may not be totally respected\(^6\).

4.4.2.5. System security

![Diagram](image)

**Figure 74: Allowed delays in reporting events – System security**

Each data source, must protect the data that it contains to prevent unauthorized access. This requirement applies during the buffering and transmitting processes as well as during the regular data access cycle. The network packets containing the data being reported must also be protected as a security breach at this point could easily propagate corrupted information\(^6\).

**Guarantee of control to the access to the data feeding process:** Option D1, has a high level of security, once having to feed near real-time data, almost no or very little data is retained in a buffer area, thus, prevents security violation action as such as data modification or data access. In option D2, the security level is medium, once having one day time lag to report events, the buffer area can become vulnerable to external attacks. In option D3, the security level is low, once having one week time lag to report events, the buffer area can become very vulnerable to external attacks.

**Guarantee of a secure data feeding process:** In terms of data transmitting process the three options face the same optimal level of security, as any moving data through a network must use secure, authenticated, and industry-accepted encryption mechanisms and order security initiatives as such, data should be encrypted via application level, data traffic must be transmitted over Secure Sockets Layer (SSL)\(^6\), using only strong security

---


Implementation analysis of a EU system for traceability and security features of tobacco products
Interim Report II

4.4.2.6. Potential of reducing illicit trade

One of the key elements in EU’s strategy to fight the illicit trade of tobacco is to have a stronger enforcement of tax, customs, police and border authorities. For example, this includes further joint customs operations, providing technical and financial assistance to Member States and non-EU countries to strengthen their capacities, enhance the exchange of information at EU and international level between the actors concerned especially the cooperation with major source and transit countries; setting up of a new independent laboratory for the analysis of cigarettes. Taking that into account, each option presents a distinct potential of reducing illicit trade:

In option D1, the potential is very high, once having access to near real-time data, actions can be taken right after the event being reported and data analytics systems based on incident detection can help to prevent illicit trade when providing near real-time data to tax, customs, police and border authorities. In option D2, the potential is lower when compared with option D1, once allowing the Competent Authorities to have access to the data that is almost one day old, actions can be taken only after that time lag. In option D3, the potential is very low, once allowing the Competent Authorities to have access to one week old data, actions can be taken only after that time lag, which indeed, for example, is possible to become extremely late in case an action must be taken prior a product being delivered.

67 Fighting the illicit trade of tobacco products - http://ec.europa.eu/anti-fraud/strategies/tobacco/files/docs/body/q_and_a_en.pdf
4.4.2.7. Burden for economic stakeholders

![Pie charts showing burden for economic stakeholders for options D1, D2, and D3]

Figure 76: Allowed delays in reporting events – Burden for economic stakeholders

The Burden for the economic operators, for each option are very similar, where all options demand the adaption of their systems and processes, software development, data integration and hardware acquisition. All three options differ when regarding the period of data retention and the risk of operations halting.

Data Capture, Compilation and Transmitting: As explained before, the process of an event reporting must be accomplished within the maximum allowed delay, which includes: the whole process of data capture, any internal data processing needs and/or intermediary steps through the management systems (WMS, MES, ERP, UTrack), then finally the report of the event data to the Tracking and Tracing system. The option D1 has a higher impact on the economic operator when regarding the necessary time to capture and compile relevant data prior being transmit.

Local Buffer Area for Temporary Data Retention and Process Decoupling: Prior being reported to the Tracking and Tracing system, the data is retained in a local buffer area, first-of-all used to decouple the production process from the data reporting process, and secondly to keep the data stored prior being reported. The buffer area needs can highly increase depending on the period of the retention.

In option D1, the score positively high, concluded to a lower period of data retention, directly impacting on the local buffer, which can be very small and less demanding, therefore the option presents a low burden for the economic stakeholder, whereas the other options, as the data retention time increases, the operation complexity also increases, reflected on the growth of the volume of data to be processed and transmitted in a more concentrated time period. For instance, when having one week time lag, the volume of data captured during this time can be thousand times bigger than when reporting on option D1, therefore, the volume of the retained data highly increases for option D3.

It is important to notice that, both options D2 and D3 also have negative impacts on their scores due to the risk of imposing the distribution/logistic operations to be halted, in case of no full report are available for the Competent Authorities for the purpose of spot.

---

68 Data Collection, Compilation and Dissemination - [link](http://www.tffs.org/pdf/method/2013/psds13ch6.pdf)
Regardless of the option chosen, it is always considered that generating the security features will always imply a minor impact on the manufacturers' production process (e.g. the option may add an activity to the process, but does not limit its speed).

When considering the production and application of the security features, option ‘(S1) Affixing’ is the best of the three. Given that the majority of most Member States (22 out of 28) currently use fiscal marks (i.e. tax stamps), the manufacturers of tobacco products already have practice at managing and affixing paper stamps or labels.

On the other hand, when considering the outsourcing of the security features, and although most tax stamps are currently manufactured by a third party managed by the Member States authorities, and then transported to the manufacturers of tobacco products, the reality is that a direct printing allows for the security features to be integrated in the commercial package, which eliminates the impact on the manufacturers production process.

Apart from these minor impacts, all options are technically feasible, and no one is excluded from the selection process because of this selection criteria.

4.5.2.2. Interoperability (with key users’ and other company’s systems)

All three options guarantee a full interoperability with the systems of key users and other systems of the economic operators.

For the key users, regardless of which option is chosen, the relationship between the national authorities and the Commission should be guaranteed, as should the exchange of information regarding new security threats.

Interoperability with other company’s systems only applies if the security elements selected have some digital features that may have to be integrated with the company’s systems.

And even if this integration is necessary, all three options are fully capable of doing so, as it will be function of the specific digital element considered, and not of the chosen method of application.

![Figure B2: Method of adding a security feature – Interoperability (with key users’ and other company’s systems)](image)
counterfeited product, and give it the impression of being legal, whilst for printed security features, anyone attempting to circumvent the system will have more difficulty in doing so.

Again, the differences presented will affect the choice of the policy option, but they do not reach a level that would disqualify any option at this point.

### 4.5.2.5. System security

For ‘System security’, all options generate some risk to the overall security of the system.

![Figure 85: Method of adding a security feature – System security](image)

Although security measures can be implemented to improve the security of the production environment, the transport and the storage of the security features (and the necessary supplies to produce and apply the security features), there is always at least a minor risk of having a security breach.

The security of the system should be considered of the utmost importance; and these risks, although minor at this stage, are real in the majority of supply chains, and shall also apply to tobacco products, as they present high revenues to illicit traders.

### 4.5.2.6. Potential of reducing illicit trade

Given the risks presented before, options ‘(S2) Printing or integrating through a different method’ or ‘(S3) Any method’ are considered to have a perfect score on the ‘Potential to reduce illicit trade’. This is not true, however, for option ‘(S1) Affixing’.

![Figure: Method of adding a security feature – System security](image)
When '(S1) Affixing', even with the utilisation of frangible paper, that makes the paper stamps used both tamper proof and irremovable, there is always a higher risk of circumventing the system.

One of the largest criticisms to this method, regardless of the scope of application, is the fact that an affixed solution secures only itself, and not the product it is applied to. As previously noted, and with the high revenues generated by the illicit trade of tobacco products, one needs to take extra care when affixing security features onto unit packets of tobacco products.

4.5.2.7. Burden for economic stakeholders

The 'Burden for economic stakeholders' is viewed as the costs that are being applied to economic stakeholders. In this case, and since the costs are limited to the application of security features onto unit packets of tobacco products, the burden is limited to the Tobacco Manufacturers/Importers that are placing the products on the EU market.

Regarding the three options proposed, the overall evaluation is as follows.

The complete cost analysis of the different alternatives may be found in Annex 8.5 Method of adding a security feature.

4.5.2.8. Burden for public authorities

Regarding the 'Burden for public authorities', all options reach a perfect score. The justification for this is simple: no costs are being applied to the public authorities.
When evaluating the criteria, one must consider that this policy option deals only with the method of adding a security feature. All the controls performed by the public authorities are considered under decision point A. Governance model.

It is also possible for Member States to aggregate the security features with the national tax stamps (where applicable), as envisaged in the Article 16 of the TPD. However, this is a choice of each Member State, which falls off the scope of this exercise.

**4.5.3. Conclusion - Selected alternative**

When considering all selection criteria, and the weighting defined, the final results point to option '(S3) Any method' as the best way to add a security feature onto unit packets of tobacco products.

This means that Member States’ authorities, and Tobacco Manufacturers, can choose between options '(S1) Affixing' and '(S2) Printing or integrating through a different method,' depending on the requirements of the Member States and on the type of tobacco product considered. It is important to note at this stage that both options S1 and S2 scored very high too, and are in fact very close to what is considered the optimal solution (being that the optimal solution is a combination of options S1 and S2, the proximity in the results is to be expected).

This is in line with the required flexibility in the application of security features. As long as the security elements proposed comply with the requirements of Article 16 of the TPD, any method of application can be considered.
This also takes into account the possibility for Member States to combine the security features with their tax stamps (where applicable). This opens the possibility to minimise the burden of the Member States on the application of tax stamps, while being fully compliant with the TPD.

When analysing all the selection criteria, it’s important to note that all options defined secured a perfect score on the primary requirements defined by Chafea. On the secondary (or optimisation) requirements, however, there are several differences that can be noted. Option S3 appears at the top of the majority of selection criteria presented, but is many times accompanied by the other options considered.

The main differences occur on the ‘Burden for economic stakeholders’, where a somewhat large gap between option 1 and options 2 and 3 created some relevant differences in the scoring of that criteria.

Figure 90: Method of adding a security feature – Comparison of the score of the secondary requirements
5. **General Concept of the System**

The general concept of the system is a combination of all the evaluation carried out regarding each alternative policy option. This way, the proposed optimal system is as presented below.

<table>
<thead>
<tr>
<th>Who?</th>
<th>Tracking and Tracing</th>
<th>Security features</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) Governance model</td>
<td>(B) Data storage model</td>
<td>(C) Allowed data carriers</td>
</tr>
<tr>
<td>(A1) Industry operated solution</td>
<td>(B1) Centralised model</td>
<td>(C1) System with a single data carrier for all identification levels</td>
</tr>
<tr>
<td>(A2) Third party operated solution</td>
<td>(B2) Decentralised model as per Manufacturer/Importer</td>
<td>(C2) System with a single data carrier per identification level and optional data carriers for aggregation packaging levels</td>
</tr>
<tr>
<td>(A3) Mixed solution (industry and third party)</td>
<td>(B3) Decentralised model as per Member State</td>
<td>(C3) System with limited variety of data carriers for all identification levels</td>
</tr>
<tr>
<td></td>
<td>(B4) Combined model: centralised for surveillance and decentralised for recording as per Manufacturer/Importer</td>
<td>(C4) System with limited variety of data carriers for all identification levels and optional data carriers for aggregation packaging levels</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>(C5) Free system allowing any existing approved data carrier</td>
</tr>
</tbody>
</table>

Table 8: Optimal system based on the alternative policy options

The evaluation of the alternative policy options (chapter 4) contains all the justifications for this solution. A more detailed evaluation can be found on annex A.

The optimal system proposed aims to achieve a full compliance with Articles 15 and 16 of the TPD and Article 8 of the FCTC Protocol, while ensuring maximum efficiency to the lowest costs possible. The general concept of the system is presented below, according to the defined:

- Business Process Diagram;
By reducing the supply of under-priced illicit cigarettes, and using price elasticity estimates, a reduction in smokers is expected. In addition, academic literature proposes a corresponding decrease of expected Non-Communicable Diseases (NCD), with an associated reduction in the NCD economic burden for the 28 Member States.

- Increased fiscal revenues
  - For each percentage of the current tobacco market that is illicit, a potential tax loss amount can be calculated. Again, depending on price elasticity estimates, tax benefits of implementing the solution can be estimated, given the levels of impact that the solution can have on illicit trade.

From a qualitative perspective, a decrease in the availability of illicit tobacco can result in consumers smoking less or quitting smoking altogether. If there is a reduction in consumption this could mean less absenteeism from work and a decrease in the number of people retiring early, due to smoking-related health issues. Furthermore, a reduction in smoking will impact the life expectancies of smokers.

The benefits of the solution will be mainly focused on the quantitative perspective. However, the qualitative perspective will also be estimated, with values for all 28 Member States.

Below are the annualised baseline benefits of the solution, in million euros. The detailed analysis of the benefits generated by the solution can be found on Annex C: Detailed Calculation of the Benefits.

<table>
<thead>
<tr>
<th>Year</th>
<th>New tax revenues from VAT</th>
<th>New tax revenues from other taxes</th>
<th>Reduction in healthcare expenditure</th>
<th>Total public benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>397.62</td>
<td>1 156.21</td>
<td>59.02</td>
<td>1 612.85</td>
</tr>
<tr>
<td>2</td>
<td>397.62</td>
<td>1 156.21</td>
<td>59.02</td>
<td>1 612.85</td>
</tr>
<tr>
<td>3</td>
<td>397.62</td>
<td>1 156.21</td>
<td>59.02</td>
<td>1 612.85</td>
</tr>
<tr>
<td>4</td>
<td>397.62</td>
<td>1 156.21</td>
<td>59.02</td>
<td>1 612.85</td>
</tr>
<tr>
<td>5</td>
<td>397.62</td>
<td>1 156.21</td>
<td>59.02</td>
<td>1 612.85</td>
</tr>
</tbody>
</table>

Table 10: Overall benefits of the solution (million €)

5.1.2.4. Costs

The cost analysis was performed as part of the evaluation of each alternative policy option. In this section, a summarised view of the annualised costs of the whole solution is presented, taking into account both “one off” costs and “recurring” costs, in order to enable a comparison of the benefits generated by its implementation. The costs are presented in million euros.

<table>
<thead>
<tr>
<th>Year</th>
<th>(A) Governance model</th>
<th>(B) Data storage model</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>86.76</td>
<td>5.59</td>
</tr>
<tr>
<td>2</td>
<td>86.76</td>
<td>5.59</td>
</tr>
<tr>
<td>3</td>
<td>86.76</td>
<td>5.59</td>
</tr>
<tr>
<td>4</td>
<td>86.76</td>
<td>5.59</td>
</tr>
<tr>
<td>5</td>
<td>86.76</td>
<td>5.59</td>
</tr>
</tbody>
</table>

Price elasticity is a measure used in economics to show the responsiveness, or elasticity, of the quantity demanded of a good or service to a change in its price. More precisely, it gives the percentage change in quantity demanded in response to a one percent change in price (which is the reason why price elasticity is almost always negative – when increasing the price, the demand tends to decrease).
The detail of the costs presented here can be found on Annex B: Detailed Calculation of the Costs.

When analysing the detailed costs, it is necessary to take into account that for the evaluation of the alternative policy options, all costs related with that option were taken into account, without looking at synergies with the other decision points.

### 5.1.3. Conclusion

The costs of the solution are considerable, but it is important to notice that the solution has the potential to generate a large set of benefits for the Member States, and for its citizens.

The following table shows the benefits assuming a 30% reduction in contraband, 10% in counterfeit and 10% in cheap whites – our baseline situation. With this assumption, the potential benefits generated practically double the baseline costs of the overall solution.

<table>
<thead>
<tr>
<th>(C) Allowed data carriers</th>
<th>137.64</th>
<th>137.64</th>
<th>137.64</th>
<th>137.64</th>
<th>137.64</th>
</tr>
</thead>
<tbody>
<tr>
<td>(D) Allowed delays in reporting events</td>
<td>59.64</td>
<td>59.64</td>
<td>59.64</td>
<td>59.64</td>
<td>59.64</td>
</tr>
<tr>
<td>(E) Method of adding a security feature</td>
<td>75.57</td>
<td>75.57</td>
<td>75.57</td>
<td>75.57</td>
<td>75.57</td>
</tr>
<tr>
<td><strong>Total costs</strong></td>
<td><strong>365.20</strong></td>
<td><strong>365.20</strong></td>
<td><strong>365.20</strong></td>
<td><strong>365.20</strong></td>
<td><strong>365.20</strong></td>
</tr>
</tbody>
</table>

Table 11: Overall costs of the solution (million €)

When considering the differences in the options chosen from the alternative policy options, the benefits generated can drop roughly 68%, reaching a minimum value of 515.90 million euros.

This exercise can also be performed for the costs, assessing the cheapest solution possible (disregarding its potential of reducing illicit trade, or any other criteria), and the most
5.2. Business Process Diagram

The objective of the Business Process Diagram is to represent the activities of the tobacco products supply chain in their normal sequence, identifying all the actors involved and clarifying their roles.

The figure below presents a high-level view of the tobacco products supply chain, from which the business processes will be designed.

![Business Process Diagram](image)

This view can still be "drilled-down" up to a point where the main sub-processes of the tobacco products supply chain can be identified:

![Detailed Process Diagram](image)
After this high-level view, the rest of this chapter will be approached at a detailed level, as we will detail down until we reach an “activity” level, due to the relevance of identifying the exact points where, for instance, to capture the unique identifiers and their related data.

Due to the complexity of covering all possible cases in all countries and economic stakeholders, the business process will be defined in a generic way, in which all industry actors can be represented and can identify themselves. The notation used will follow the Business Process Model and Notation (BPMN) standard, which is easy to understand for a non-IT audience.

The main elements produced in the definition of the business processes are:

- Process diagram, according to BPMN standard;
- Process activities, with:
  - Description of the activity and its components;
  - Responsible for each activity;
  - Inputs and outputs of each activity;
  - Constraints associated with the execution of each activity;
- Responsibility assignment matrix per process, identifying the roles and responsibilities per each actor and activity.

For the responsibility assignment matrix, a RACI matrix is used, in which RACI stands for:

---

70 Object Management Group; “A standard Business Process Model and Notation (BPMN) provides businesses with the capability of understanding their internal business procedures in a graphical notation and gives organizations the ability to communicate these procedures in a standard manner. Furthermore, the graphical notation facilitates the understanding of the performance collaborations and business transactions between the organizations. This will ensure that businesses will understand themselves and participants in their business and will enable organizations to adjust to new internal and B2B business circumstances quickly”; http://www.bpmn.org/
Very often the role that is accountable for a task or deliverable may also be responsible for completing it (indicated on the matrix by the task or deliverable having a role accountable for it, but no role responsible for its completion (i.e. it is implied)). Outside this exception, it is generally recommended that each role in each activity receive, at most, just one of the participation types.

The Business Process Diagrams for the business processes identified previously are modelled according with the BPMN standard. The detailed Business Process Diagrams can be found on annex D.

### 5.3. System Architecture

This section describes the high-level system architecture of the Track and Trace system. The system architecture is based on the business processes, detailed in section 10.1 Business Process Diagram. The system architecture represents and describes the main components and interfaces that comprise the Track and Trace system.

#### 5.3.1 Use case diagram

This section introduces the use case diagram of the Track and Trace system. The use case diagram is introduced as a transition diagram, between the business view (i.e. business process diagrams) and the system architecture diagrams, to facilitate the understanding.

The purpose of the use case diagram is to provide a high-level view of the system and convey a simplified and graphical representation of what the Track and Trace system shall actually do. The use case diagram is a representation of the users’ interaction with the Track and Trace system that shows the relationships between the different types of...
Therefore, at the highest level, the Track and Trace system will comprise the following sub-systems:

- An independent central **Surveillance system**, which offers a secure unique access point to a **global comprehensive view** of the traceability and trade data based on the data hosted locally. This data has been previously synchronised from the distributed Data Storage systems. Prior to such synchronisation, the Data Storage systems have conducted specific verifications to assure the integrity of that data. Moreover, the Surveillance system includes the interfaces needed to accommodate the integration with key users’ systems (i.e. ECMS or SEED).

- A group of **Data Storage systems**, which behave as **intermediate layers focused on data management and storing**. Each Data Storage system manages data exclusively related to a certain (or group of) manufacturer(s)/importer(s). This data management conducts specific data integrity checks, which are necessary prior to the consolidation of any new record notified by the economic operators. In order to accomplish such verifications, these integrity checks only need to access to the data repository hosted locally, of a certain (or group of) manufacturer(s)/importer(s). Once the data integrity is successfully verified and it is consolidated into the local Data Storage repository, it is synchronised with the Surveillance system immediately. Moreover, each Data Storage system includes the interfaces needed to accommodate the integration with the Competent Authorities.

The high-level system architecture of the Track and Trace system is depicted as follows, based on the standard UML component diagram notation:\(^72\):

![Figure 98: High-level system architecture diagram](image)

---

Firstly, the group of Data Storage systems are fed with data received from the following sources:

- A specific (or group of) manufacturer(s)/importer(s) that have concluded contracts to establish this storage facility.

- A (or group of) independent UID Generator(s). When the (or group of) third party UID Generators(s) deliver the UIDs requested by the manufacturer, the UIDs *have to* be notified also to the Data Storage system.

- The Surveillance system itself when routing the traceability and trade reporting events from the economic operators. The Surveillance system offers a central secure routing service, which decouples the client reporting systems of being aware of the Data Storage systems' location, simplifying the configuration and operational processes of the wholesalers and distributors (i.e. wholesalers and distributors actually are dealing with tobacco products from different manufacturers).

Secondly, when the data managed by the Data Storage systems is successfully consolidated and has overcome the integrity checks, it is promoted to the Surveillance system through a synchronisation process. Hence, the Surveillance system is fed exclusively with data received from the group of Data Storage systems. To that end, the Surveillance system should *be connected with* the Data Storage systems with adequate communication backbone network *in order to* ensure secure data transfer and minimise the network latency.

Finally, both the Surveillance and the Data Storage systems publish interfaces to the Competent Authorities and the External Auditors.

### 5.3.2.1. Software interfaces

Prior to the specification of the software interfaces, the following remarks shall be considered:

- Technical details of the data types, models and communication protocols will be provided in Work Package 3. Nevertheless, the catalogue includes a preliminary list of the alternatives to be considered in Work Package 3.

- The specifications of the interfaces, data models and communication protocols shall be *based on standards, or open equivalent, to the greatest extent possible*. Standards promote interoperability, enable the system to be future-proof and cost effective, and allow for open and fair competition between providers and stakeholders avoiding monopolistic situations. A standard based system would facilitate the integration with external systems such as the European Excise Movement and Control System (EMCS) or international implementations of the FCTC Protocol. If current standards do not fulfil entirely the Tracking and Tracing current needs, it is recommended to try to extend state of the art standards where possible and appropriate.

- **According to** the information needs specified by the TPD, it can be derived that two *data categories* shall be transmitted and recorded in the Data Storage system, as a minimum:
  - **Traceability data**, which is referred in Art. 15(5) as the entry, intermediate movements and final exit of all unit packets into the possession of any economic operator involved in the trade of tobacco products.
Trade data, which is referred in Art. 15(2)(j) and Art. 15(2)(k) as the trade information involved in any transaction (i.e. purchaser, the invoice, order number and payment records of all purchasers from manufacturing to the first retail outlet).

These data categories are exchanged as events that shall include time-stamp information that helps establishing a consistent temporal order on these time-stamps. This is of paramount importance because the inherent nature of the Track and Trace system is totally distributed, and the transmission of data from the remote sources (i.e. manufacturers and economic operators) may not happen in real-time. As such, events may be not received in the Data Storage system in the same temporal order in which they occurred and application specific integrity checks are necessary and shall be conducted prior to the data consolidation.

As discussed above, these data categories shall be based on open standards such as ISO/IEC 19987:2015 EPC Information services - Specification. Currently, this standard is widely adopted by the supply chain industry to share data. This open standard specifies an abstract data model to exchange supply chain specific data (i.e. trade information, traceability information, and logistics information). This abstract data model is based on XML, so it can be extended through the creation of specific profiles. Moreover, this standard specifies different communication bindings. Finally, it should be noted that this standard does not impose any specific database implementation and is based on the EPC Information System (EPCIS) GS1 standard version 1.1.

5.3.2.1.1. Interfaces published by the Surveillance system

The catalogue of software interfaces, published by the Surveillance system, is as follows:

<table>
<thead>
<tr>
<th>Interface S2CAS</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>S2CAS</td>
<td>Surveillance to Competent Authorities client System</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Owner System</th>
<th>Data Source</th>
<th>Data Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surveillance system</td>
<td>Surveillance system</td>
<td>Competent Authorities' client systems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Data Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceability</td>
<td>To be defined.</td>
</tr>
<tr>
<td>Trade</td>
<td></td>
</tr>
<tr>
<td>Mater data (e.g. UIDs at packet level, UIDs of aggregation levels, manufacturers identifiers, facilities identifiers, etc.)</td>
<td>Alternatives to consider:</td>
</tr>
<tr>
<td></td>
<td>GS1 standards for identification 75.</td>
</tr>
</tbody>
</table>

---

75 GS1 Standards for identification – [http://www.gs1.org/id-keys](http://www.gs1.org/id-keys)
A frame element represents a consistent place providing a graphical boundary for the interaction. In addition to providing a visual border, the frame element also has an important functional use in diagrams depicting interactions.

In this diagram two types of frames are used:

- **alt**: Alternatives are used to designate a mutually exclusive choice between two or more message sequences, allowing the model to represent the classic "if then else" logic.

The word "alt" is placed inside the frame at the top left corner. The larger rectangle is then divided into operands, separated by a dashed line. Each operand is given a guard to test against.

- **strict**: Strict sequencing fragment (denoted "strict") encloses a series of messages which must be processed in the given order.

Comments regarding the interaction, positioned next to the referred item.

| Table 12: Sequence Diagrams – Legend |

At the top, the lifelines represent each one of the objects that interacts between them:

- The Independent Third Party UID Generator
- The Tobacco Manufacturer/Importer
- The internal Local Buffer Area Data Storage
- The Tracking and Tracing System Decentralised Data Storage
  - In the instance of no Decentralised Data Storage, all its interactions shown on the sequence diagram, should be shifted to the Tracking and Tracing System Surveillance Data Storage lifeline.
- The Tracking and Tracing System Surveillance
- The Competent Authorities
- The Distributors/Wholesalers
- External Auditors

The interaction between the Manufacturer/Importer and the Data Storage, are always intermediate through the Local Data Storage Buffer, in order to decouple the production process from the event reporting process.

The Tracking and Tracing System Decentralised Data Storage is synchronized with the Tracking and Tracing System Surveillance in a regular basis, as previously explained on the Data Storage Model and on the System Architecture sections. This synchronization process is not depicted on the sequence diagram because its frequency is unbound from the interactions, thus, do not represent an interaction in this sequence.
5.5. Data Flow Diagram

The diagram below presents the data flow interaction between the External Entities, the Processes and the Data Repositories, on a high-level view of the system.

Every data flow is detailed defined in the Business Process Diagram.

The interaction sequence arrow depicted on the sequence diagram shown on the previous section. The interfaces are depicted on the section System Architecture Diagram.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>Process</td>
<td>Is any process or task that is performed by the system</td>
</tr>
<tr>
<td>Data Storage</td>
<td>Data Storage</td>
<td>Is a place where data is held between processes</td>
</tr>
<tr>
<td>External Entity</td>
<td>External Entity</td>
<td>Is any initial source of data or any final destination for processed data</td>
</tr>
<tr>
<td>Arrow</td>
<td>Arrow</td>
<td>Is the direction of the data flow between a source and a destination</td>
</tr>
</tbody>
</table>

Table 13: Data Flow Diagrams – Legend
6. Conclusion

Interim Report II is the major output of Work Package 2 and represents a major milestone in the project, as it includes the high-level design of the optimal system, which will then be specified during the course of Work Package 3.

For this purpose, the first part of the report focuses on the definition and characterisation of all alternative policy options under evaluation for the Tracking and Tracing system, and the Security features applied to unit packets of tobacco products. These options are based on what was proposed under the Inception Impact Assessment, and were refined with our expertise and knowledge gathered during the implementation of Work Package 1.

The objective of this first part is to ensure a clear understanding of all options considered, in order to serve as the basis for evaluation.

On the second part of the report, all the options defined are evaluated against a set of selection and evaluation criteria. The selection criteria compose the high-level requirements of the system, and can be divided as:

- Primary requirements, or the mandatory requirements that each option needs to guarantee to be considered for the optimal system (i.e. full compliance with Articles 15 and 16 of the TPD and Article 8 of the FCTC Protocol).
- Secondary requirements, or the criteria for optimisation of the system (i.e. technical feasibility, interoperability (with key users’ systems and other company’s systems), ease of operation, system integrity, system security, potential of reducing illicit trade, burden for economic stakeholders, and burden for public authorities).

These selection criteria, however, are not enough to evaluate each alternative policy option. For that purpose, a set of evaluation criteria was defined. The evaluation criteria were defined and scored for each alternative policy approach, which enables us to have a score per selection criteria. The selection criteria are then weighted to add up each individual contribution to the overall score of the alternative policy options.

These two steps – definition and evaluation – summarise the process used to evaluate each alternative policy option. Starting from the alternative policy options, we needed to drill down until a lower level to be able to properly evaluate each option, and then rolled back up to have results per selection criteria, and ultimately, a total score for each alternative policy option.

The results of this evaluation compose the suggested high level optimal system, as presented below.