Document 12.2 **Pages 1 to 34 were entirely redacted as they fall outside the scope of the request**

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

4.1.1.5. Assumptions

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

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

4.1.1.6. Constraints

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

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

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

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

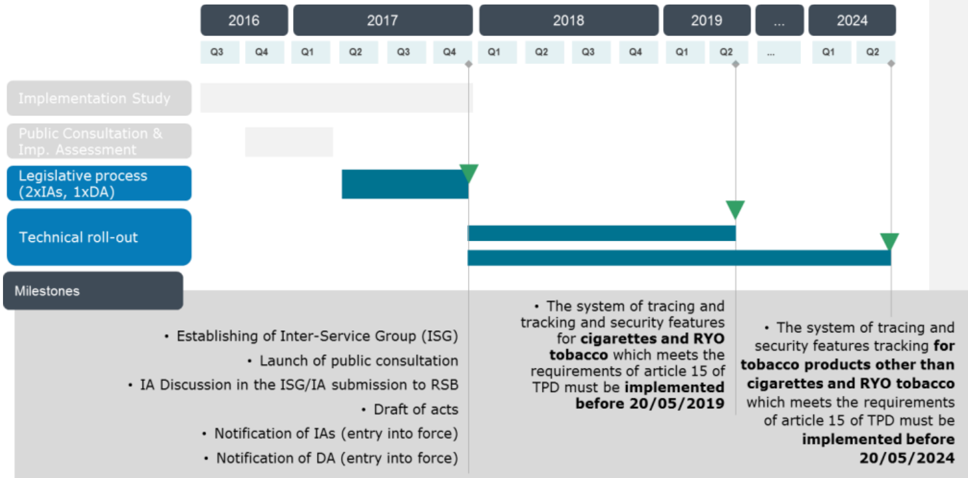
4.1.1.7. Roadmap

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

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

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

Commented[redacted]: I assume that at the beginning of the technical roll-out in 2018 a more detailed map of milestones will be created. E.g. selecting and approving of the different providers of systems must be done in Q1/Q2



- Establishing of Inter-Service Group (ISG)
- Launch of public consultation
- IA Discussion in the ISG/IA submission to RSB
- Draft of acts
- Notification of IAs (entry into force)
- Notification of DA (entry into force)

- The system of tracing and tracking and security features for **cigarettes and RYO tobacco** which meets the requirements of article 15 of TPD must be **implemented before 20/05/2019**

- The system of tracing and security features tracking **for tobacco products other than cigarettes and RYO tobacco** which meets the requirements of article 15 of TPD must be **implemented before 20/05/2024**

4.1.2. Governance and stakeholders

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

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

Commented[redacted]**:** In my opinion not only advised but **crucial** to the success of the system.

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

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

The allocation should be as follows:

Pages 37 to 41 were entirely redacted as they fall outside the scope of the request

Figure 12: Combined model: centralised for surveillance and decentralised for recording

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

This option enables the economic operators to choose between an authorised variety of data carriers for the unit packet and all aggregation packaging levels, where the data carriers for each identification level may differ.

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

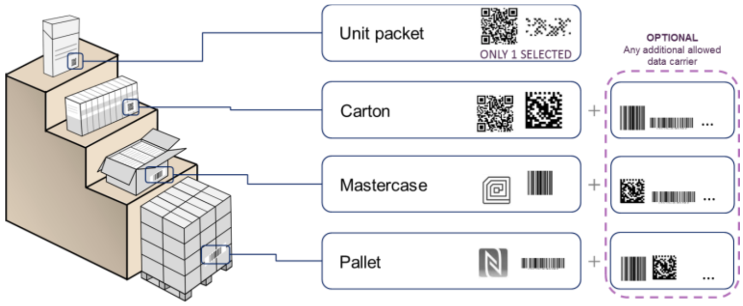


Figure 13. Description of the system with limited variety of data carriers per identification level and optional data carriers for aggregation packaging levels

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

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

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

- A low-latency business enterprise. The economic operator production line and data transmit channels must be able to access, propagate and process the data in low latency. That means that any approval or confirmation of the event is done through management software (such as an ERP), and the event reporting must be concluded within this allowed delay.
- A continual input and output of data being processed in a short period of time (near real-time).
- A highly fault-tolerant reporting system on the economic operators' side, with the ability to recover from data report process failure, in order to keep the same level of performance and deal with any unforeseen problems, such as connection downtimes.

Commented [redacted]: I think any chosen system needs to be (highly) fault-tolerant. Highly in this means the system needs to be able to fix issues faster.

Pages 43 to 53 were entirely redacted as they fall outside the scope of the request

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

Table 20: Directive 2014/40/EU requirements

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

- **Length of the unique identifier**. A code with such a high number of data elements is not a common practice in the industry. The optimal size of the unique identifier to be applied to a unit packet of tobacco products should not exceed 60 characters and preferably be closer to 40 characters. Otherwise, the negative impact on high-speed production lines will be significant.
- **Access to legible information** for competent authorities. The elements that form the unique identifier can be previously encoded to reduce the length of the unique identifier. This enhances the use of lookup tables as an instrument to decode and to convert the codes into legible information for competent authorities, increasing the effectiveness of surveillance activities.

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

The steps of this analysis are:

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

Structure of the unique identifier

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

Commented [redacted]**:** Where is the calculation method for the verification digit? Will this be described in an additional (low-level) technical document?

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

Pages 55 to 78 were entirely redacted as they fall outside the scope of the request

data analytics while also supporting high rates of message throughput for input/output operations.

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

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

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

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

Commented [redacted]**:** I assume this is part of authentication and authorisation roles to view data.

Page 80 was entirely redacted as it falls outside the scope of the request

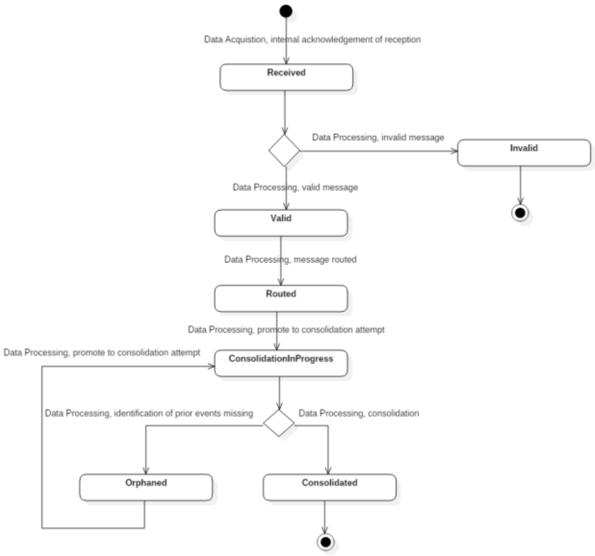

Data Acquistion, internal acknowledgement of reception
Received
Data Processing, invalid message
Invalid
Data Processing, valid message
Valid
Data Processing, message routed
Routed
Data Processing, promote to consolidation attempt
Data Processing, promote to consolidation attempt
ConsolidationInProgress
Data Processing, identification of prior events missing
Data Processing, consolidation
Orphaned
Consolidated

Figure 33: Event state diagram

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

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

Commented [redacted]]: What is a "standard interface", it's a broad term? It leaves the solution providers in al MS open to use all kinds of interfaces as long as the canonical data model is implemented.

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

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

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

Pages 82 to 112 were entirely redacted as they fall outside the scope of the request