



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

Final Report

Annex II – Technical Specifications of the Tracking and Tracing System and the Security Features

Service Contract N° 2015 71 05



an NTT DATA Company

everis
April 2018

Public
Health

EUROPEAN COMMISSION

Consumers, Health, Agriculture and Food Executive Agency
Health Unit

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

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

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

*European Commission
B-1049 Brussels*

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

Final Report

Annex II – Technical Specifications of the Tracking and Tracing System and the Security Features

Service Contract N° 2015 71 05

***Europe Direct is a service to help you find answers
to your questions about the European Union.***

Freephone number (*):

00 800 6 7 8 9 10 11

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

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

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

Luxembourg: Publications Office of the European Union, 2018

PDF	ISBN 978-92-9200-875-8	doi:10.2818/343517
-----	------------------------	--------------------

© European Union, 2018

Reproduction is authorised provided the source is acknowledged.

TABLE OF CONTENTS

0. INTRODUCTION	9
1. GENERAL ELEMENTS OF THE TRACKING AND TRACING SYSTEM	10
1.1. Process map	10
1.2. Registration processes	11
1.2.1. Registration	11
1.2.2. Correction of information.....	12
1.2.3. De-registration.....	14
1.3. Business process diagrams	15
1.3.1. General view.....	17
1.3.2. Processes diagrams and activities.....	17
1.4. System users	54
1.4.1. RACI matrix.....	54
1.4.2. System user details	59
1.5. Use cases	62
1.5.1. Audit of data storage	62
1.5.2. Notify	64
1.5.3. Risk-based surveillance	65
1.5.4. Data access by manufacturers and importers.....	67
1.5.5. Query data	68
1.6. Control mechanisms	74
1.7. Contingency plans	86
1.7.1. Introduction.....	86
1.7.2. Concept of operations	87
1.7.3. Activation and notification	88
1.7.4. Recovery.....	89
1.7.5. Reconstitution.....	98
1.8. System security plan	100
1.8.1. Introduction.....	100
1.8.2. Scope	100
1.8.3. Security needs	101
1.8.4. Proposed methodology	103
1.8.5. Candidate security requirements	105
2. DETAILED TECHNICAL SPECIFICATIONS FOR THE SUPPLY CHAIN ELEMENTS OF THE TRACKING AND TRACING SYSTEM.....	107
2.1. Unique identifier (at unit packet level)	107
2.1.1. Assessment of the requirements and composition of the unique identifier	107
2.1.2. Requirements specification	122
2.2. Unique identifier (at aggregation packaging level)	124
2.2.1. Assessment of the requirements and composition of the unique identifier	124
2.2.2. Requirements specification	130
2.3. Data carrier (at unit packet level).....	132
2.3.1. Preliminary analysis.....	132
2.3.2. Analysis for the selection of data carriers	135
2.3.3. Technical requirements	139
2.4. Data carrier (at aggregation packaging level).....	139
2.4.1. Analysis for the selection of data carriers	139

2.4.2. Technical requirements	141
3. DETAILED TECHNICAL SPECIFICATIONS FOR THE IT ARTEFACTS OF THE TRACKING AND TRACING SYSTEM	142
3.1. System Architecture	142
3.1.1. Requirements specification	142
3.1.2. Architectural goals.....	142
3.1.3. Architectural decisions	143
3.1.4. Overview diagram	147
3.2. Sequence diagrams	152
3.2.1. Request for serial number	153
3.2.2. Event reporting	156
3.2.3. Data outbound	158
3.2.4. Data auditing.....	159
3.3. Data flow diagram	160
3.4. Temporary Buffer (optional component).....	161
3.4.1. Recommendation on the requirements to be accomplished	161
3.5. Message.....	164
3.5.1. Requirements specification	164
3.5.2. Format specification.....	167
3.6. System users.....	201
3.6.1. Definition	201
3.6.2. Responsibilities (Roles)	202
3.6.3. Permissions (Rights).....	204
3.6.4. Role-permission	205
3.6.5. User-role.....	205
3.7. Primary Data Storage	205
3.7.1. Requirements specification	206
3.8. Surveillance Data Storage	220
3.8.1. Requirements specification	220
3.9. Repository Router.....	236
3.9.1. Requirements specification	236
3.10. System for the issuance of unique identifiers	239
3.10.1. Requirements specification	239
3.11. Data Dictionary	249
3.11.1. Registered entities.....	249
3.11.2. Lookup entities to support the decoding of the unique identifier elements	249
3.11.3. Canonical data model.....	250
3.11.4. Data dictionary technical details	251
3.12. Common validation rules for the data.....	270
3.13. Security policy	272
3.14. Confidentiality policy.....	275
3.15. Contingency plan.....	275
4. GLOSSARY AND TERMS OF REFERENCE	278
5. BIBLIOGRAPHY.....	279

TABLE OF FIGURES

Figure 1: General view of the tobacco products supply chain	15
Figure 2: General view of the tobacco products supply chain – Manufacture/ Import.....	16
Figure 3: General view of the tobacco products supply chain – Distribute	16
Figure 4: RACI matrix definition	54
Figure 5: Methodological approach for the codification of the unique identifier	107
Figure 6: Methodological approach for the codification of the unique identifier at aggregation packaging level.....	125
Figure 7: System overview diagram.....	147
Figure 8: High-level system architecture diagram.....	150
Figure 9: Medium-level components’ architecture diagram	152
Figure 10: User-role, role-permission and role-role relationships representation.....	202
Figure 11: Canonical data model entity diagram.....	250
Figure 12: Event state diagram	265
Figure 13: Unique identifier state diagram.....	269

TABLE OF TABLES

Table 1: Directive 2014/40/EU requirements	108
Table 2: Lookup table description	109
Table 3: Analysis of the elements of information	110
Table 4: Example of location of manufacturing activities code	112
Table 5: Example of lookup table for location of manufacturing activities.....	112
Table 6: Example of code for unit packet identification	114
Table 7: Example of lookup table for product description.....	114
Table 8: Example of code for manufacturing timestamp	115
Table 9: Example of code for shipment route information	116
Table 10: Example of lookup table for shipment route.....	116
Table 11: Example of code for importer into the Union.....	118
Table 12: Example of lookup table for importers	118
Table 13: Example of ID Issuer identification code	119
Table 14: Example of code for serial number	120
Table 15: Coding format of the unique identifier at a unit packet level	122
Table 16: Summary of the lookup table's size	122
Table 17: Example of location of aggregation activities code.....	126
Table 18: Example of lookup table for location of aggregation activities	127
Table 19: Example of code for date and time of aggregation activities	127
Table 20: Example ID Issuer identification code	127
Table 21: Example of code for serial number	129
Table 22: Example of location of manufacturing activities code	130
Table 23: Summary of the lookup tables size.....	130
Table 24: Categories of data carriers	133
Table 25: Typical usage of data carriers	134
Table 26: Preliminary selection of data carriers	135
Table 27: Data carriers analysis for Category 1 of tobacco products.....	136
Table 28: Data carriers analysis for Category 2 of tobacco products.....	136
Table 29: Data carriers analysis for Category 3 of tobacco products.....	137
Table 30: Data carriers analysis for Category 4 of tobacco products.....	138
Table 31: Allowed data carriers for unit packet of tobacco products	138
Table 32: Data carriers analysis for Category 1 of aggregation packaging.....	139
Table 33: Data carriers analysis for Category 2 of aggregation packaging.....	140
Table 34: Allowed data carriers for aggregation packaging levels of tobacco products	141
Table 35: Architectural decision - Repository Router	145
Table 36: Architectural decision – Canonical data model.....	147
Table 37: Tracking and Tracing System interfaces	151
Table 38: Types of messages to be exchanged through the Tracking and Tracing System.....	168

0. INTRODUCTION

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

The present document is the Annex II of the study carried out, and is complemented by:

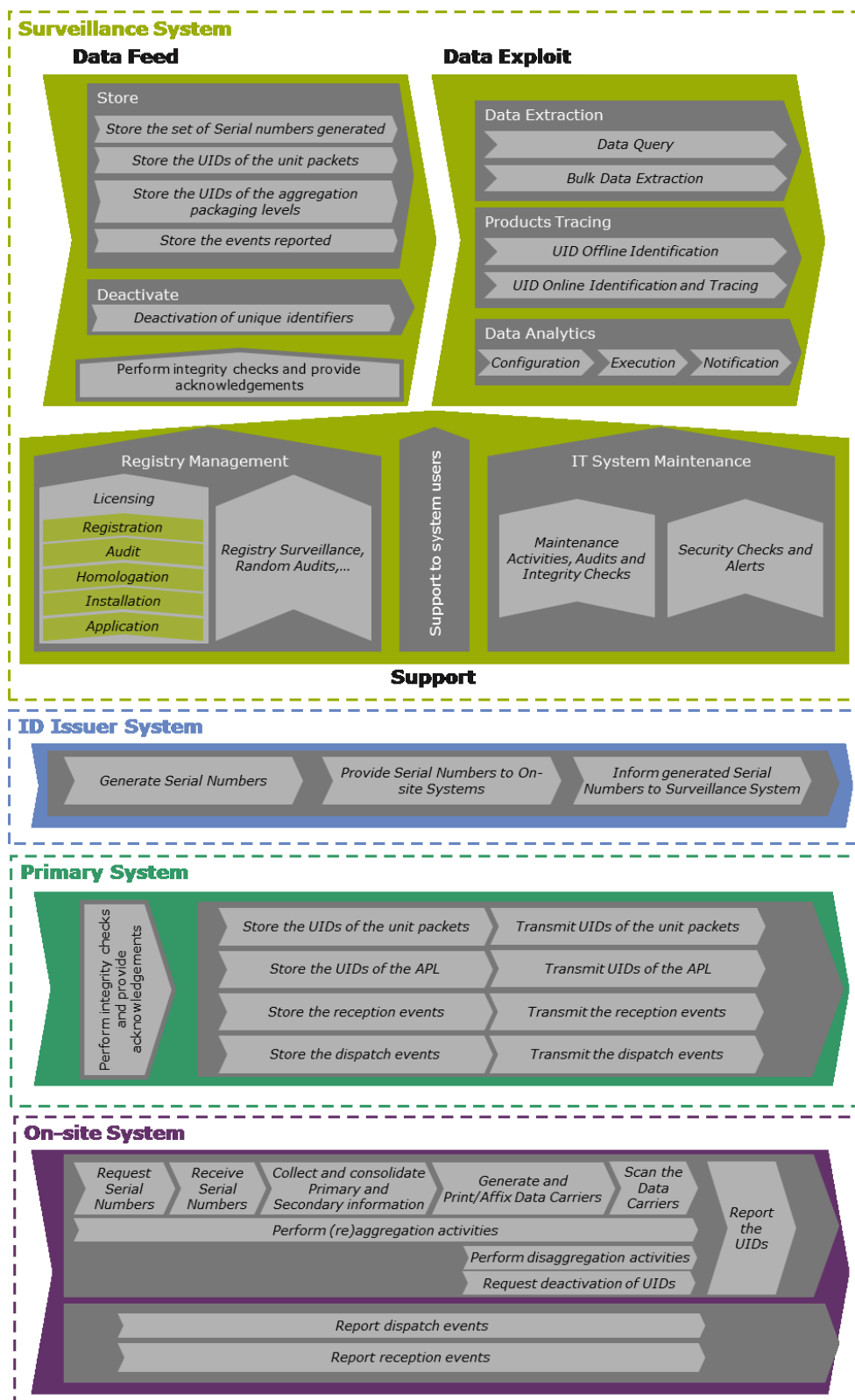
- Main Report
- Annex I – Evaluation of Policy Options
- Annex III – Model Contract

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

Volume	Catalogue number	ISBN	DOI
Main Report	EB-02-17-895-EN-N	978-92-9200-770-6	10.2818/453932
Annex I – Evaluation of Policy Options	EB-02-17-896-EN-N	978-92-9200-874-1	10.2818/628162
Annex III – Model Contract	EB-02-17-898-EN-N	978-92-9200-876-5	10.2818/751591

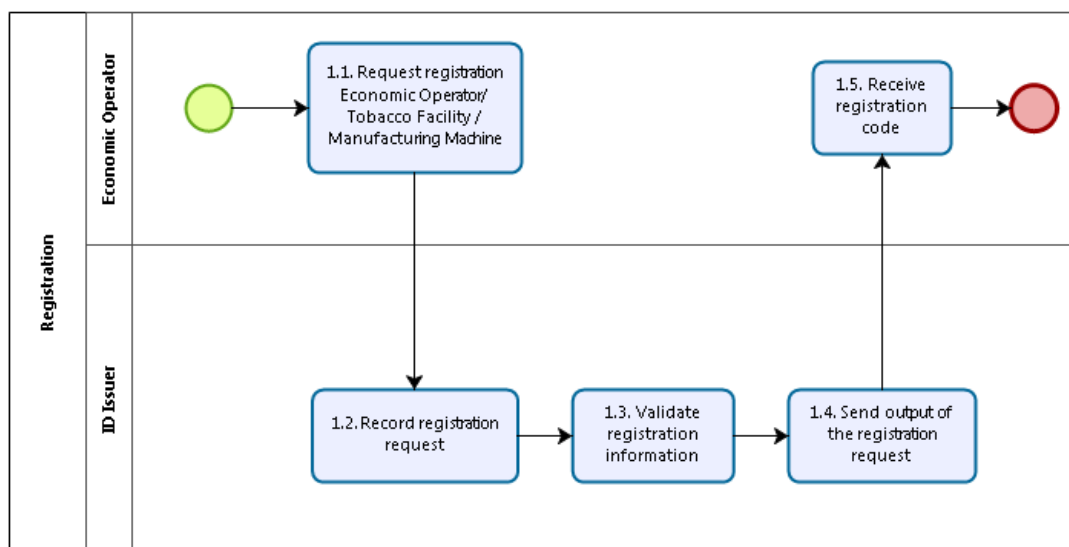
1. GENERAL ELEMENTS OF THE TRACKING AND TRACING SYSTEM

1.1. Process map



1.2. Registration processes

1.2.1. Registration



Activity 1.1. Request registration of the economic operator/tobacco facility/manufacturing machine

Description	Responsible
Economic operator(s) send a message to the ID Issuer to request registration of the economic operator / tobacco facility / manufacturing machine	<ul style="list-style-type: none"> Economic operator(s)
Inputs	
<ul style="list-style-type: none"> N/A 	
Outputs	
<ul style="list-style-type: none"> Registration request 	

Activity 1.2. Record registration request

Description	Responsible
ID Issuer receives and records the registration request and the information sent along with it	<ul style="list-style-type: none"> ID Issuer
Inputs	
<ul style="list-style-type: none"> Registration request 	
Outputs	
<ul style="list-style-type: none"> N/A 	

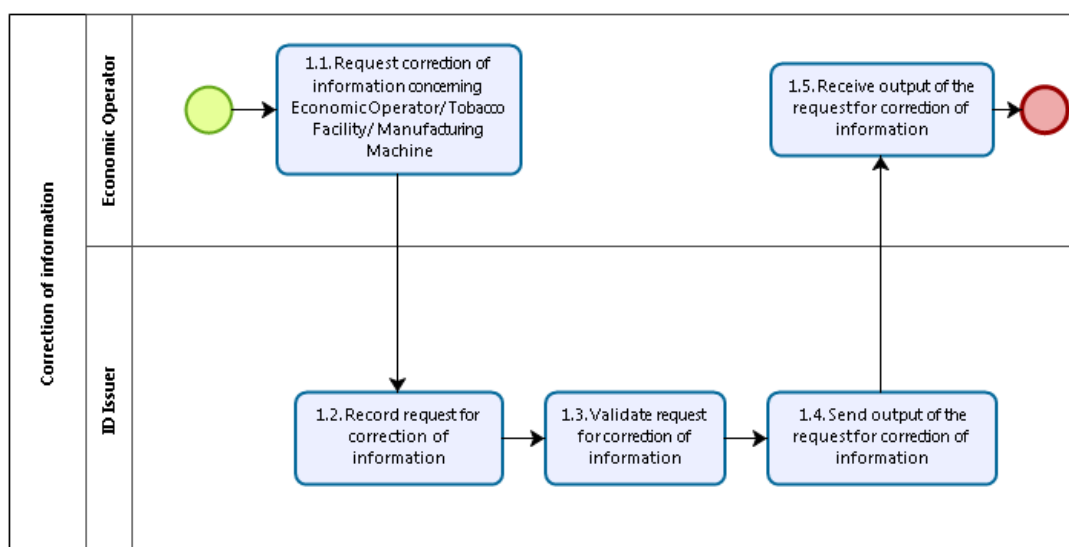
Activity 1.3. Validate registration information

Description	Responsible
ID Issuer validates the information received in the registration request	<ul style="list-style-type: none"> ID Issuer
Inputs	
<ul style="list-style-type: none"> N/A 	
Outputs	
<ul style="list-style-type: none"> N/A 	

Activity 1.4. Send output of the registration request	
Description	Responsible
ID Issuer, after validation of the information received in the request for registration, sends the output of the registration request to the economic operator(s) (EO_ID, EO_CODE / F_ID / M_ID)	<ul style="list-style-type: none"> ID Issuer
Inputs	
<ul style="list-style-type: none"> N/A 	
Outputs	
<ul style="list-style-type: none"> EO_ID, EO_CODE / F_ID / M_ID 	

Activity 1.5. Receive registration code	
Description	Responsible
The economic operator(s) receive the output of the registration request sent by the ID Issuer after validation of the request	<ul style="list-style-type: none"> Economic operator(s)
Inputs	
<ul style="list-style-type: none"> EO_ID, EO_CODE / F_ID / M_ID 	
Outputs	
<ul style="list-style-type: none"> N/A 	

1.2.2. Correction of information



Activity 1.1. Request correction of information concerning the economic operator/tobacco facility/manufacturing machine	
Description	Responsible
Economic operator(s) send a message to the ID Issuer to request for correction of information concerning the economic operator / tobacco facility / manufacturing machine	<ul style="list-style-type: none"> Economic operator(s)
Inputs	
<ul style="list-style-type: none"> N/A 	
Outputs	

- Request for correction of information

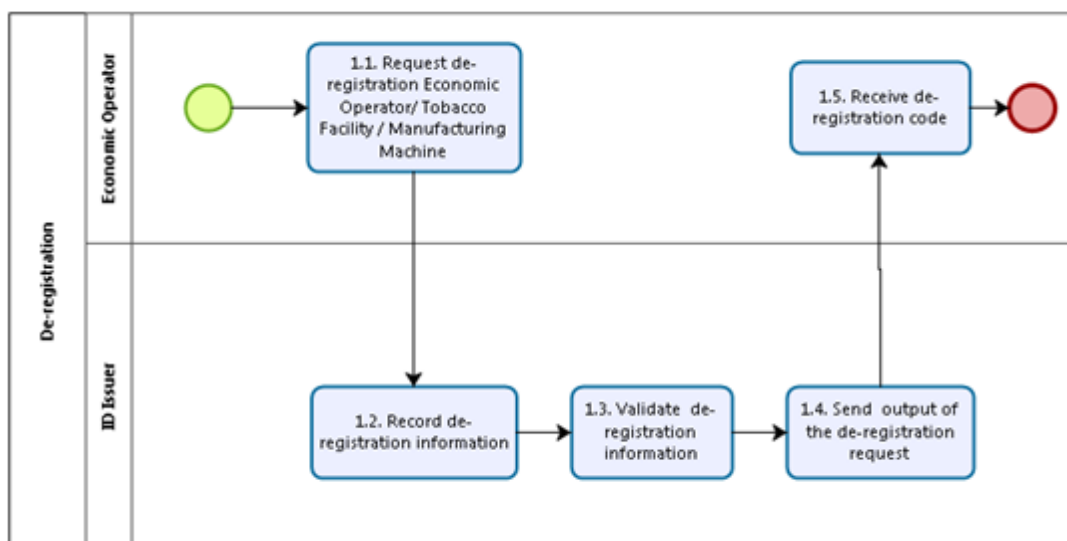
Activity 1.2. Record request for correction of information	
Description	Responsible
ID Issuer receives and records the request for correction of information and the information sent along with it.	<ul style="list-style-type: none"> ▪ ID Issuer
Inputs	
<ul style="list-style-type: none"> ▪ N/A 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 1.3. Validate request for correction of information	
Description	Responsible
ID Issuer validates the information received in the registration request	<ul style="list-style-type: none"> ▪ ID Issuer
Inputs	
<ul style="list-style-type: none"> ▪ N/A 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 1.4. Send output of the request for correction of information	
Description	Responsible
ID Issuer, after validation of the information received in the request for correction of information, sends the output of the request for correction of information to the economic operator(s) (EO_ID, EO_CODE / F_ID / M_ID)	<ul style="list-style-type: none"> ▪ ID Issuer
Inputs	
<ul style="list-style-type: none"> ▪ N/A 	
Outputs	
<ul style="list-style-type: none"> ▪ EO_ID, EO_CODE / F_ID / M_ID 	

Activity 1.5. Receive output of the request for correction of information	
Description	Responsible
The economic operator(s) receive the output of the request for correction of information sent by the ID Issuer after validation of the request	<ul style="list-style-type: none"> ▪ Economic operator(s)
Inputs	
<ul style="list-style-type: none"> ▪ EO_ID, EO_CODE / F_ID / M_ID 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

1.2.3. De-registration



Activity 1.1. Request de-registration of the economic operator/tobacco facility/manufacturing machine

Description	Responsible
Economic Operator(s) send a message to the ID Issuer to request for de-registration of the economic operator / tobacco facility / manufacturing machine	<ul style="list-style-type: none"> Economic operator(s)
Inputs	
<ul style="list-style-type: none"> N/A 	
Outputs	
<ul style="list-style-type: none"> De-registration request 	

Activity 1.2. Record de-registration request

Description	Responsible
ID Issuer receives and records the de-registration request and the information sent along with it	<ul style="list-style-type: none"> ID Issuer
Inputs	
<ul style="list-style-type: none"> De-registration request 	
Outputs	
<ul style="list-style-type: none"> N/A 	

Activity 1.3. Validate de-registration information

Description	Responsible
ID Issuer validates the information received in the de-registration request	<ul style="list-style-type: none"> ID Issuer
Inputs	
<ul style="list-style-type: none"> N/A 	
Outputs	
<ul style="list-style-type: none"> N/A 	

Activity 1.4. Send output of the de-registration request	
Description	Responsible
ID Issuer, after validation of the information received in the request for de-registration, sends the output of the de-registration request to the economic operator(s) (EO_ID, EO_CODE / F_ID / M_ID)	<ul style="list-style-type: none"> ID Issuer
Inputs	
<ul style="list-style-type: none"> N/A 	
Outputs	
<ul style="list-style-type: none"> EO_ID, EO_CODE / F_ID / M_ID 	

Activity 1.5. Receive de-registration code	
Description	Responsible
The economic operator(s) receive the output of the de-registration request sent by the ID Issuer after validation of the request	<ul style="list-style-type: none"> Economic operator(s)
Inputs	
<ul style="list-style-type: none"> EO_ID, EO_CODE / F_ID / M_ID 	
Outputs	
<ul style="list-style-type: none"> N/A 	

1.3. Business process diagrams

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

The Business Process Diagrams below present a general view of the tobacco products supply chain, from which the business processes will be designed.

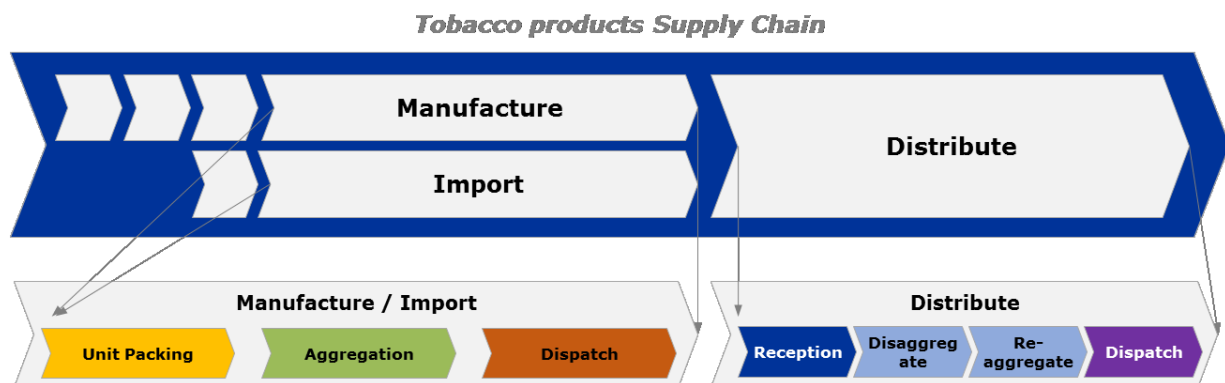


Figure 1: General view of the tobacco products supply chain

This view on the supply chain can be “drilled-down” to where the main sub-processes are identified, as in the following two figures:

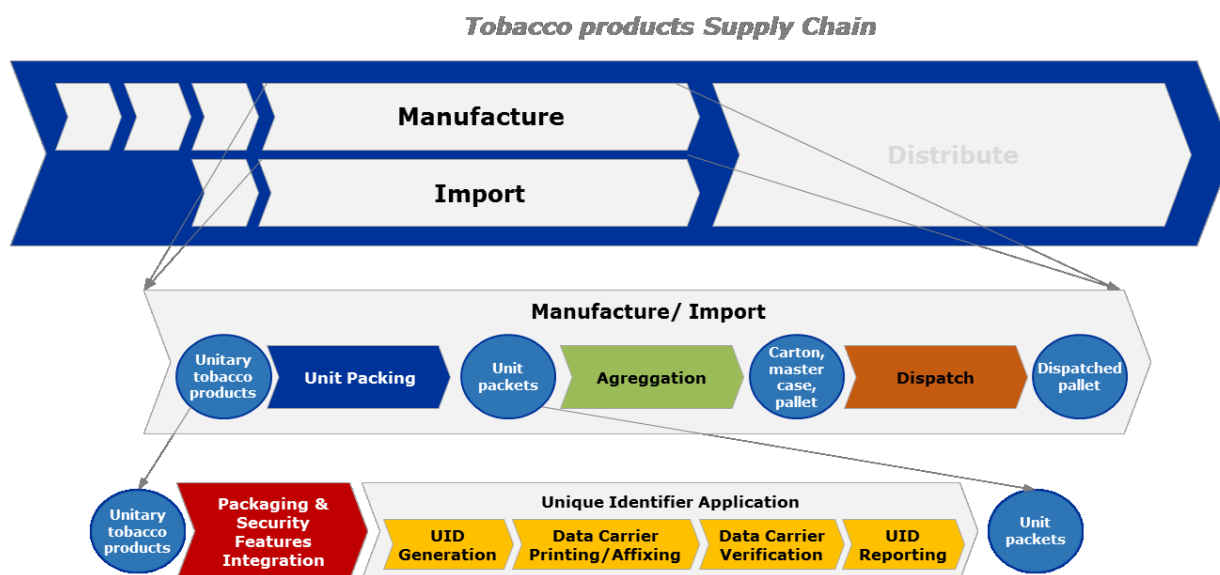


Figure 2: General view of the tobacco products supply chain – Manufacture/ Import

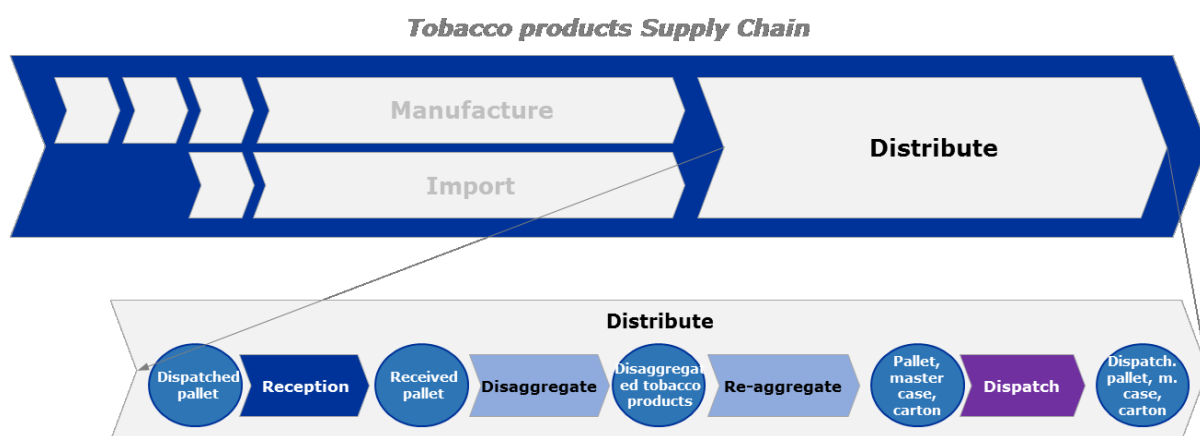


Figure 3: General view of the tobacco products supply chain – Distribute

After this general view of the tobacco products supply chain, the remainder of this chapter will provide the corresponding details of the business processes.

Due to the complexity of covering all possible cases in all Member States and for all economic stakeholders, the business processes will be defined in a generic way, through which all industry actors can be represented and can identify themselves. The notation used will follow the Business Process Model and Notation (BPMN)¹ standard, which is easily understandable for a non-IT audience.

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

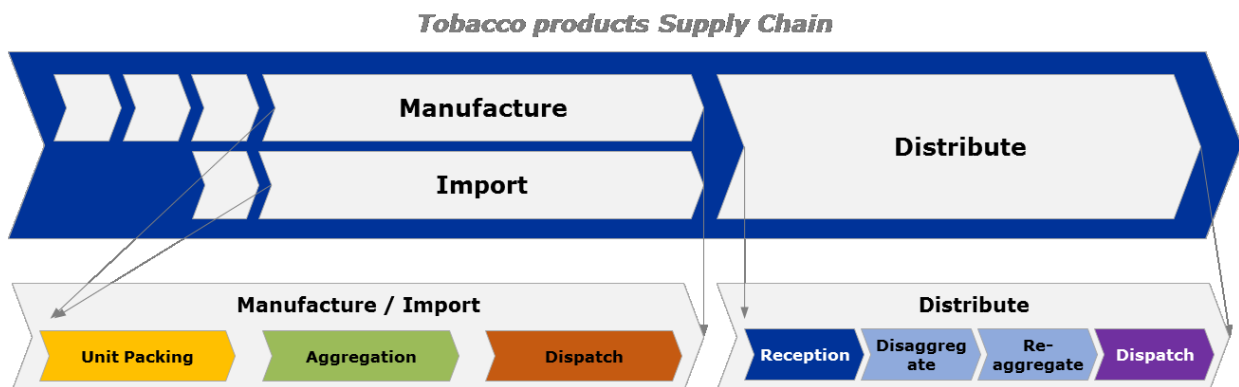
¹ Object Management Group; "A standard Business Process Model and Notation (BPMN) provides businesses with the capability of understanding their internal business procedures in a graphical notation and gives organizations the ability to communicate these procedures in a standard manner. Furthermore, 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/>

- Process diagram, following BPMN standard;
- Process activities, with:
 - Description of each activity and its components;
 - Person responsible for each activity;
 - Inputs and outputs of each activity.

The business process diagrams for the business processes previously identified are modelled according to the BPMN standard.

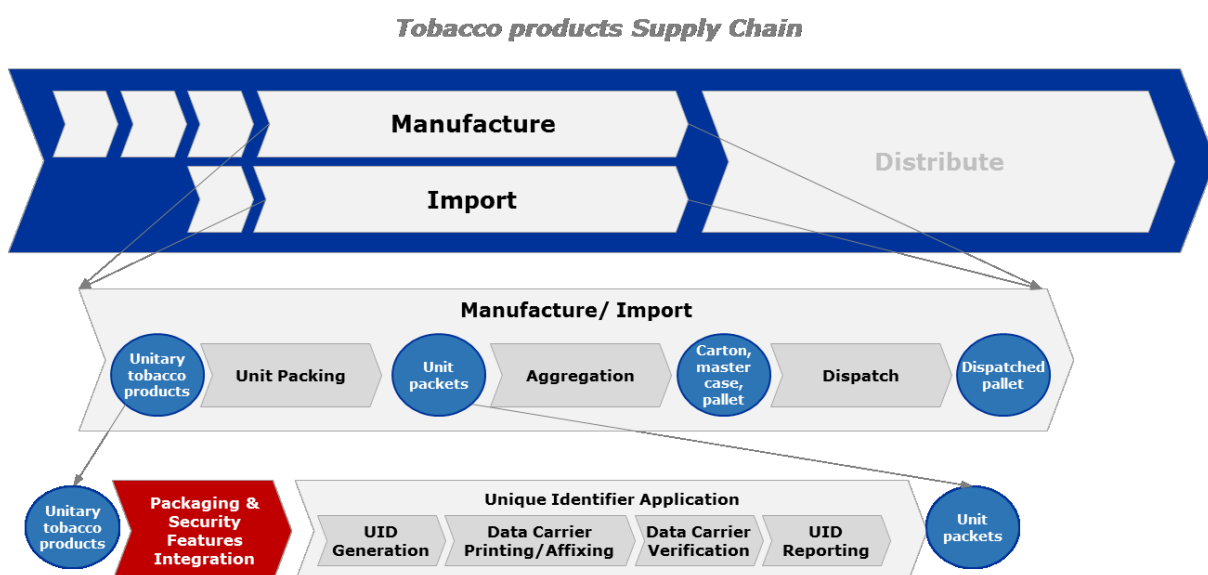
1.3.1. General view

The business process diagrams follow the same sequence as presented above, and it is possible to achieve a general view of the processes, where all the original sub-processes are identified.

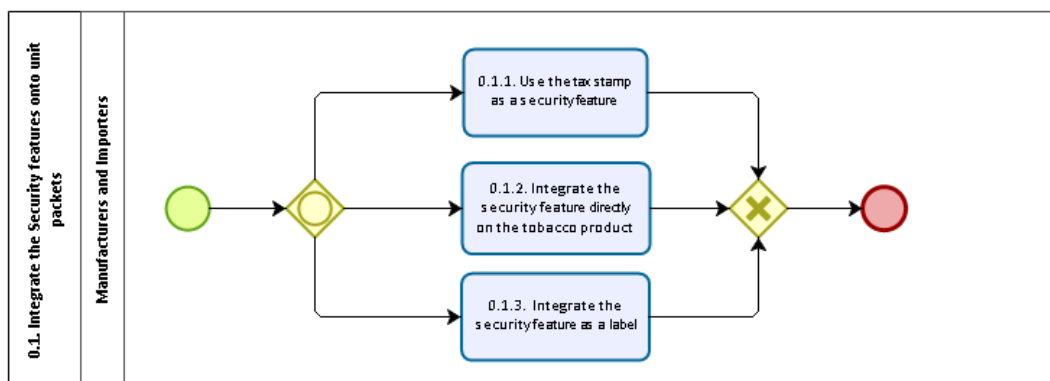


1.3.2. Processes diagrams and activities

1.3.2.1. Security features



0. Integration of a security feature



Note: Following the BPMN standard, the symbol  represents “when splitting, one or more branches are activated”, meaning that the three represented tasks can occur in parallel.

Activity 0.1.1. Use tax stamps as a security feature

Description	Responsible
<ul style="list-style-type: none"> ▪ Use tax stamps as a security feature Member States where tax stamp programmes are currently implemented use the tax stamp as a security feature. In some cases, additional features are added to tax stamps to strengthen their security, and/or meet the full requirements of the legislation. 	<ul style="list-style-type: none"> ▪ Member States are responsible for producing the tax stamp ▪ Manufacturers and importers are responsible for placing the tax stamps on the tobacco products
Inputs	
<ul style="list-style-type: none"> ▪ Tax stamps 	
Outputs	
<ul style="list-style-type: none"> ▪ Tobacco product marked with tax stamps containing the security feature 	

Activity 0.1.2. Integrate the security feature directly onto the tobacco product

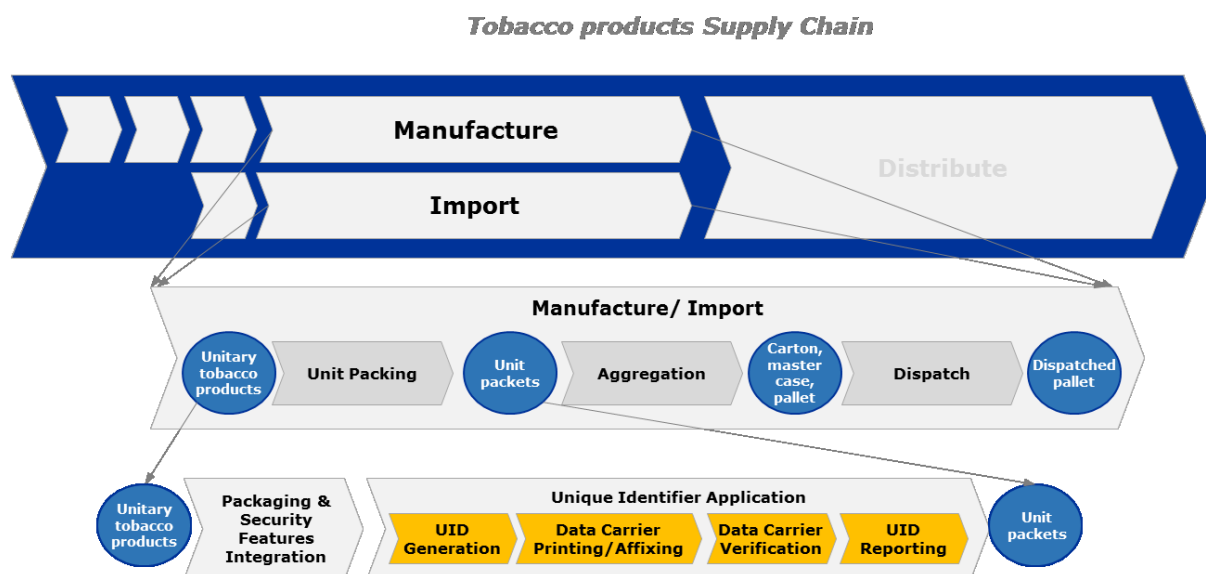
Description	Responsible
<ul style="list-style-type: none"> ▪ Integrate the security features directly onto the tobacco product In this method, the security features are integrated directly onto the tobacco product by the manufacturers and importers on the production line. 	<ul style="list-style-type: none"> ▪ Member States or an independent third party nominated by the competent authorities are responsible for the control of the integration of the security features onto the tobacco product ▪ Manufacturers and importers are responsible for the integration of the security feature onto the tobacco product
Inputs	
<ul style="list-style-type: none"> ▪ N/A 	
Outputs	

- Tobacco product with the security features directly integrated

Activity 0.1.3. Integrate the security feature as a label

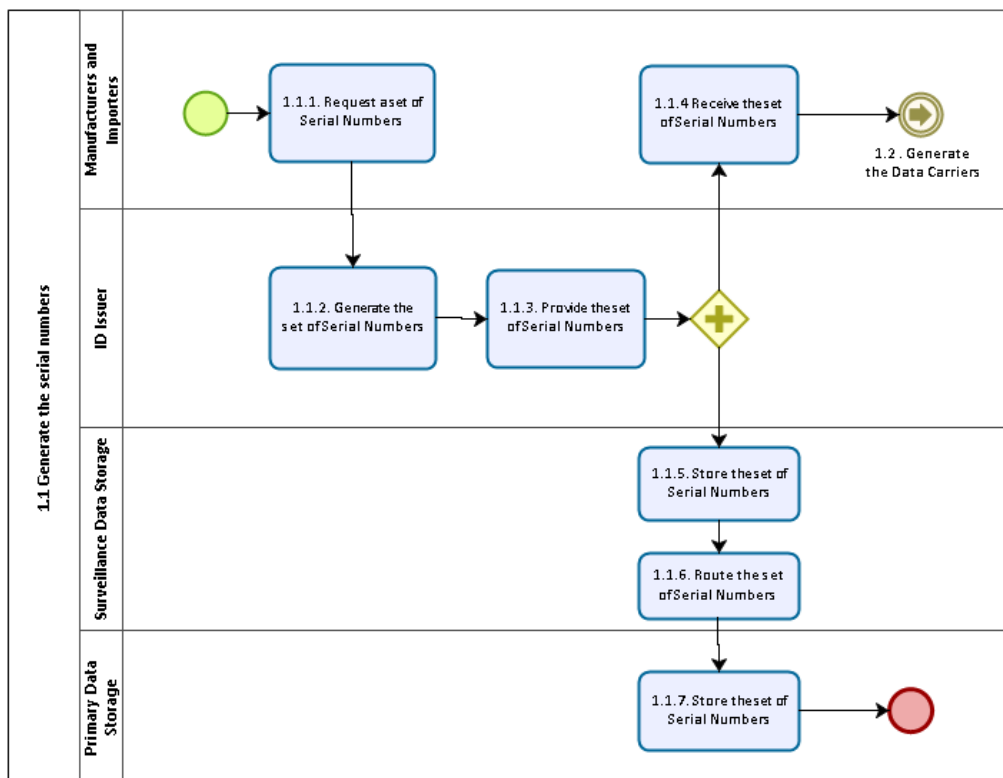
Description	Responsible
<ul style="list-style-type: none"> ▪ Integration of the security feature as a label A stamp or label is used to transport/carry the security feature comprising all of the security elements. The stamp or label is produced by a security printer, separate from the commercial processes used to produce the tobacco packaging. 	<ul style="list-style-type: none"> ▪ Member States or an independent third party nominated by the competent authorities are responsible for producing the label ▪ Manufacturers and importers are responsible for placing the label on the tobacco product
Inputs	
<ul style="list-style-type: none"> ▪ N/A 	
Outputs	
<ul style="list-style-type: none"> ▪ Tobacco product marked with a label or stamp containing the security feature. 	

1.3.2.2. Unit packets



1. UID generation

1.1 Generate the serial numbers



Activity 1.1.1. Request a set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Manufacturers and importers request a set of serial numbers (communicating 'primary information') <p>Manufacturers and importers shall communicate to the ID Issuer the request for the serial numbers they require, providing the necessary information ('primary information'): place of manufacturing, manufacturing facility, machine used to manufacture the tobacco products, product description, intended market of retail sale, intended shipment route and where applicable, the importer into the EU.</p>	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Primary information 	
Outputs	
<ul style="list-style-type: none"> ▪ Request of serial numbers with the primary information 	

Activity 1.1.2. Generate the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ▪ ID Issuer generates the set of serial numbers requested <p>The ID Issuer generates the serial numbers, according to the standards and rules defined and verifying that the request comes from an authorised (registered in the data server) entity.</p>	<ul style="list-style-type: none"> ▪ ID Issuer (under the control of the competent authorities)
Inputs	
<ul style="list-style-type: none"> ▪ Request for serial numbers ▪ Primary information 	
Outputs	
<ul style="list-style-type: none"> ▪ Sequential number issuance request ID 	

Activity 1.1.3. Provide the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ▪ ID Issuer provides the set of serial numbers requested by the authorised manufacturers and importers <p>The ID Issuer generates the serial numbers, according to the standards and rules defined.</p> <p>After the generation, the ID Issuer provides the serial numbers to tobacco manufacturers and importers, so they can proceed with the marking of the tobacco products, and to the Surveillance Data Storage.</p>	<ul style="list-style-type: none"> ▪ ID Issuer (under the control of the competent authorities)
Inputs	
<ul style="list-style-type: none"> ▪ Primary information ▪ ID Issuer identification code ▪ Set of serial numbers 	
Outputs	
<ul style="list-style-type: none"> ▪ Set of serial numbers delivered 	

Activity 1.1.4. Store the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Surveillance Data Storage receives and stores the set of serial numbers generated <p>Surveillance Data Storage receives and stores the set of serial numbers generated by the ID Issuer.</p>	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Primary information ▪ ID Issuer identification code ▪ Set of serial numbers 	
Outputs	
<ul style="list-style-type: none"> ▪ Set of serial numbers stored 	

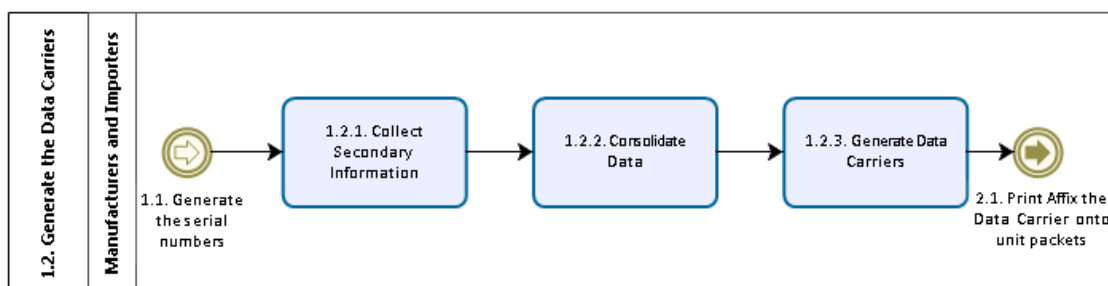
Activity 1.1.5. Receive the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Manufacturers and importers receive the set of serial numbers requested <p>Manufacturers and importers that requested sets of serial numbers receive them from the ID Issuer.</p>	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Sequential number issuance request ID 	
Outputs	
<ul style="list-style-type: none"> ▪ Set of serial numbers received. 	

Activity 1.1.6. Route the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Surveillance Data Storage routes the set of serial numbers generated <p>Surveillance Data Storage routes the set of serial numbers generated by the ID Issuer to the Primary Data Storage.</p>	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Primary information ▪ ID Issuer identification code 	

<ul style="list-style-type: none"> ▪ Set of serial numbers
Outputs
<ul style="list-style-type: none"> ▪ Primary information ▪ ID Issuer identifier ▪ Set of serial numbers

Activity 1.1.7. Store the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Primary Data Storage receives and stores the set of serial numbers generated <p>Primary Data Storage receives and stores the set of serial numbers generated by the ID Issuer.</p>	<ul style="list-style-type: none"> ▪ Primary Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Sequential number issuance request ID 	
Outputs	
<ul style="list-style-type: none"> ▪ Set of serial numbers received. 	

1.2 Generate the unique identifier and incorporate into data carriers



Activity 1.2.1. Collect 'secondary information'	
Description	Responsible
<ul style="list-style-type: none"> ▪ Collection of the 'secondary information' <p>Manufacturers and importers collect the following secondary information of each unit packet of tobacco produced or imported:</p> <ul style="list-style-type: none"> - Manufacturing timestamp 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Production / import information 	
Outputs	
<ul style="list-style-type: none"> ▪ Secondary information 	

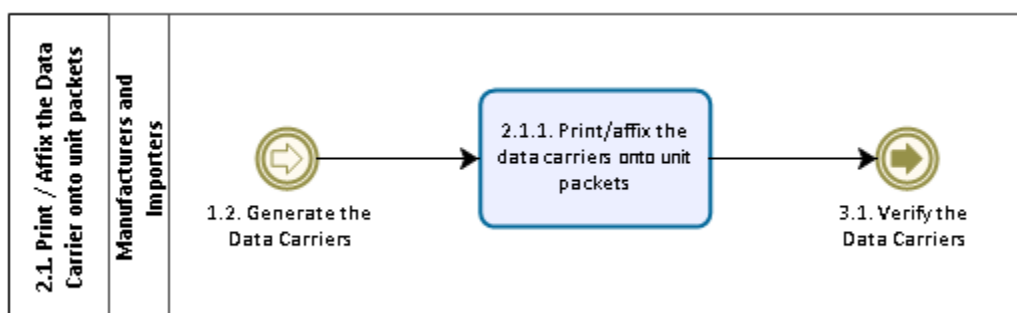
Activity 1.2.2. Consolidate data	
Description	Responsible
<ul style="list-style-type: none"> ▪ Consolidation of the serial number with the secondary information by the manufacturer/importer <p>When the manufacturers and importers receive the serial number, they consolidate all the information (primary information, ID Issuer identification code, serial number and secondary information), creating a unique identifier for each of the unit packets produced in the EU or destined for the EU market.</p>	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	

<ul style="list-style-type: none"> ▪ Primary information ▪ Serial numbers ▪ ID Issuer identification code ▪ Secondary information
Outputs
<ul style="list-style-type: none"> ▪ Unique identifier created for each unit packet

Activity 1.2.3. Generate data carriers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Generation of the data carrier The unique identifier of each unit packet is transformed into a data carrier. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifier created for each unit packet 	
Outputs	
<ul style="list-style-type: none"> ▪ Data carrier for each unit packet 	

2. Data carrier printing / affixing

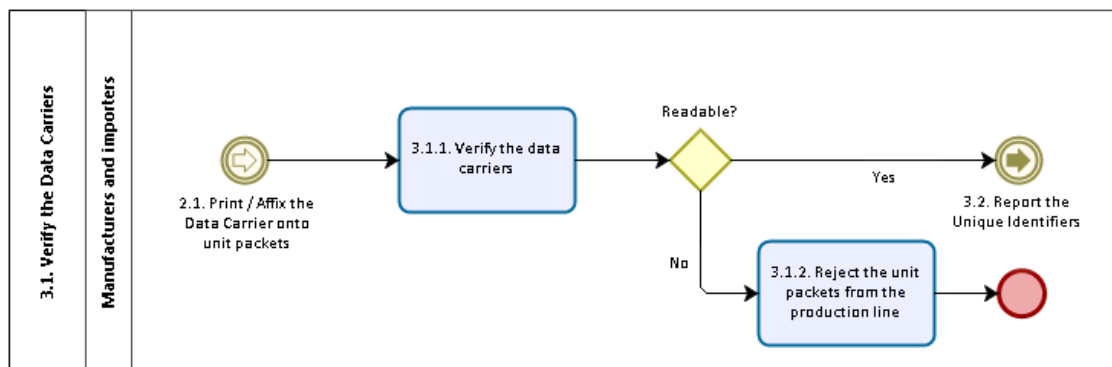
2.1. Print / affix the data carrier onto unit packets



Activity 2.1.1. Print / affix the data carrier onto unit packets	
Description	Responsible
<ul style="list-style-type: none"> ▪ Print / affix the data carrier onto unit packets When all necessary data carriers are created, the tobacco manufacturers and importers can start printing/ affixing the data carriers onto the unit packets of tobacco products. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Data carriers ▪ Unit packets 	
Outputs	
<ul style="list-style-type: none"> ▪ Unit packets marked with data carriers 	

3. Data carrier verification and unique identifier reporting

3.1. Verify the data carriers



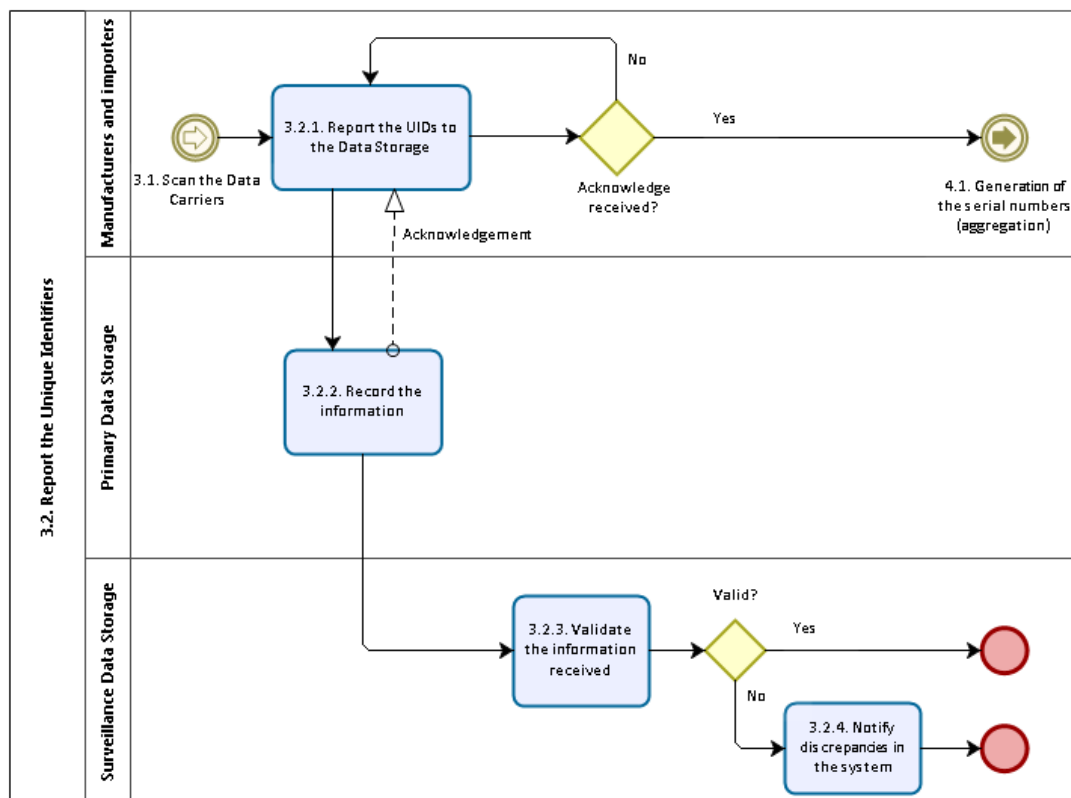
Activity 3.1.1. Scan / verify the data carriers

Description	Responsible
<ul style="list-style-type: none"> ▪ Scanning / verification of the data carriers applied The scanners must scan and read all unit packets produced on the production lines. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Unit packets marked with a data carrier 	
Outputs	
<ul style="list-style-type: none"> ▪ Unique identifiers of the data carriers 	

Activity 3.1.2. Reject the unit packets from the production line

Description	Responsible
<ul style="list-style-type: none"> ▪ Unreadable unit packets expelled from the production line If a printed data carrier is unreadable, the unit packet enters a reverse logistics procedure, in which the packet (with the data carrier) is destroyed, and the unitary tobacco products are repacked, in order to get a new unique identifier. The process of deactivation of the serial number is triggered. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Unreadable unit packets 	
Outputs	
<ul style="list-style-type: none"> ▪ Unreadable unit packets expelled from the production line 	

3.2. Report the unique identifiers



Activity 3.2.1. Report the unique identifiers to the Primary Data Storage

Description	Responsible
<ul style="list-style-type: none"> ▪ Communication to the Primary Data Storage of the data carriers scanned: serial numbers used The scanners must transmit to the Primary Data Storage all the data carriers scanned. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

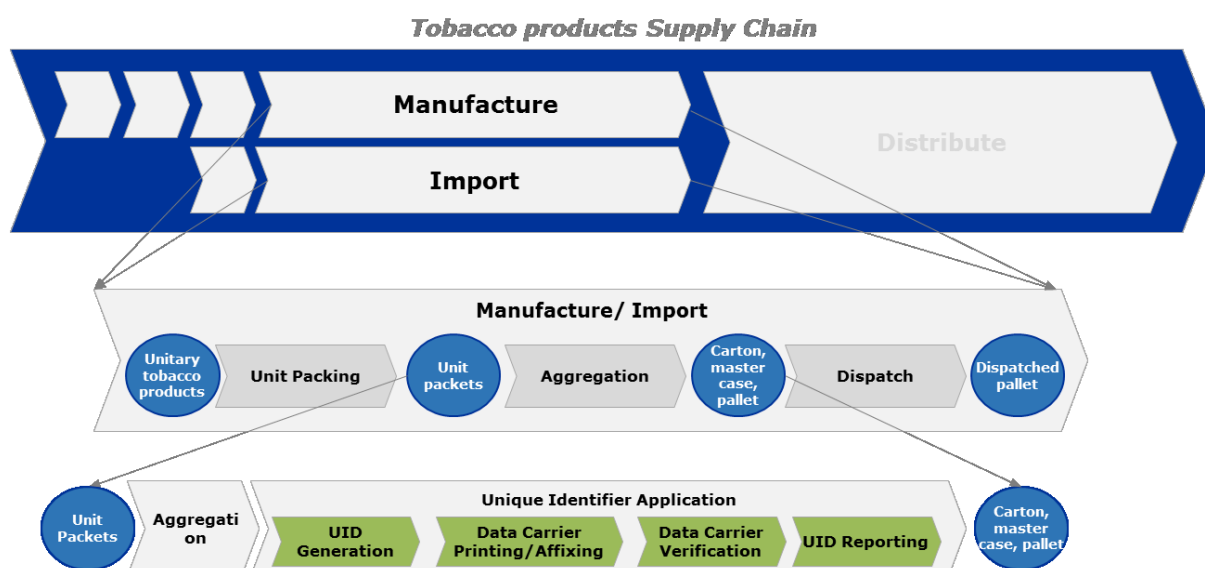
Activity 3.2.2. Record the information

Description	Responsible
<ul style="list-style-type: none"> ▪ Record the reception information After receiving the report from the manufacturers/importers, the Primary Data Storage records all unique identifiers that were reported and sends an acknowledgment to confirm that the report has been received and understood (the message is delivered in the due format and language). The retry policy, described in the Messaging Events section, applies. These records are transmitted to the Surveillance Data Storage. 	<ul style="list-style-type: none"> ▪ Primary Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 3.2.3. Validate the information received	
Description	Responsible
<ul style="list-style-type: none"> ▪ The validation of the information received comprises two stages: <ul style="list-style-type: none"> ▪ Valid unique identifiers verification (e.g. the UID has not been scanned before nor deactivated, the UID matches the information reported by the ID Issuer at the generation, the UID elements are valid, etc.). ▪ Data analytics rules verification (e.g. list of unused serial numbers or UIDs grouped per different criteria, unusual patterns in comparison with other manufacturers or importers, etc.). 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

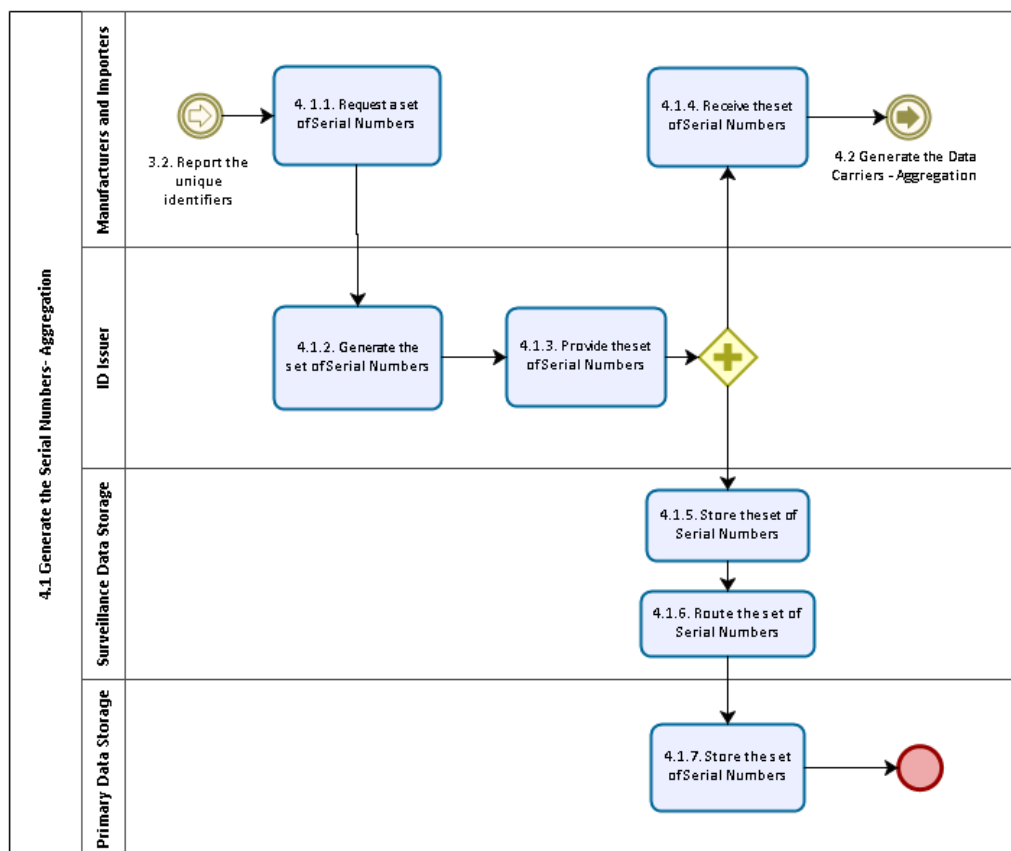
Activity 3.2.4. Notify discrepancies in the system	
Description	Responsible
<ul style="list-style-type: none"> ▪ Notification to the competent authorities if the serial number scanned cannot be found on the list of serial numbers generated (and assigned to a manufacturer/importer) <p>If the serial number scanned cannot be found on the list of serial numbers generated, a notification is sent by the Surveillance Data Storage to trigger the necessary actions.</p>	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Discrepancies found after the validation of the serial numbers by the data storage 	
Outputs	
<ul style="list-style-type: none"> ▪ Notification in case of discrepancies 	

1.3.2.3. Aggregation packaging levels



4. Unique identifier generation for aggregation packaging levels

4.1. Generate the serial numbers – aggregation



Activity 4.1.1. Request a set of serial numbers

Description	Responsible
<ul style="list-style-type: none"> Manufacturers and importers request a set of serial numbers for the aggregation packaging levels (communicating primary information) <p>Manufacturers and importers shall communicate to the ID Issuer the request for the serial numbers they require, providing the primary information: place of aggregation activities.</p>	<ul style="list-style-type: none"> Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> Primary information as described above 	
Outputs	
<ul style="list-style-type: none"> Request of serial numbers with the primary information 	

Activity 4.1.2. Generate serial numbers

Description	Responsible
<ul style="list-style-type: none"> ID Issuer generates the set of serial numbers requested for the aggregation packaging levels <p>The ID Issuer generates the serial numbers requested for the aggregation packaging levels, according to the standards and rules defined and verifying that the request comes from an authorised (registered in the data server) entity.</p>	<ul style="list-style-type: none"> ID Issuer (under the control of the competent authorities)
Inputs	
<ul style="list-style-type: none"> Request for serial numbers Primary information 	

Outputs
<ul style="list-style-type: none"> Sequential number issuance request ID

Activity 4.1.3. Provide the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ID Issuer provides the set of requested serial numbers to the authorised manufacturers and importers and to the Surveillance Data Storage <p>The ID Issuer generates the serial numbers, according to the standards and rules defined.</p> <p>After the generation, the ID Issuer provides the serial numbers to tobacco manufacturers and importers, so that they can proceed with marking the aggregation packaging levels, and to the Surveillance Data Storage for later validation.</p>	<ul style="list-style-type: none"> ID Issuer (under the control of the competent authorities)
Inputs	
<ul style="list-style-type: none"> Primary information ID Issuer identification code Set of serial numbers 	
Outputs	
<ul style="list-style-type: none"> Set of serial numbers delivered 	

Activity 4.1.4. Store the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> Surveillance Data Storage receives and stores the set of serial numbers generated by the ID Issuer for the aggregation packaging levels 	<ul style="list-style-type: none"> Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> Primary information ID Issuer identification code Set of serial numbers 	
Outputs	
<ul style="list-style-type: none"> Set of serial numbers stored 	

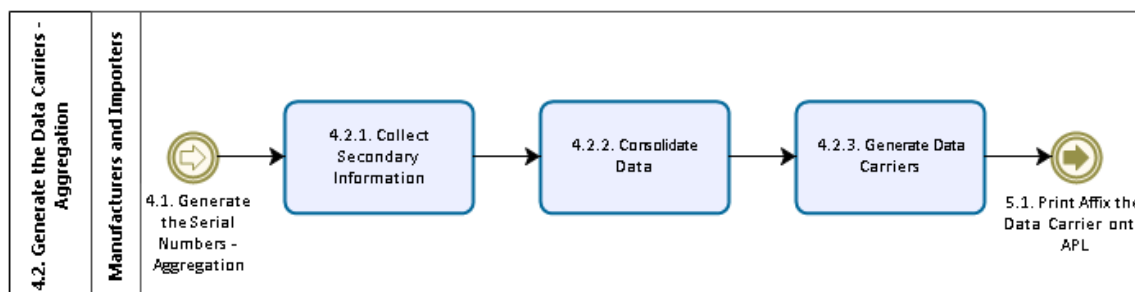
Activity 4.1.5. Receive the sets of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> Manufacturers and importers receive the sets of serial numbers requested for the aggregation packaging levels <p>Manufacturers and importers that requested sets of serial numbers for the aggregation packaging levels receive them from the ID Issuer.</p>	<ul style="list-style-type: none"> Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> Sequential number issuance request ID 	
Outputs	
<ul style="list-style-type: none"> Set of serial numbers received 	

Activity 4.1.6. Route the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> Surveillance Data Storage routes the set of serial numbers generated <p>Surveillance Data Storage routes the set of serial numbers generated by the ID</p>	<ul style="list-style-type: none"> Surveillance Data Storage

Issuer to the Primary Data Storage.	
Inputs	
<ul style="list-style-type: none"> Primary information ID Issuer identification code Set of serial numbers 	
Outputs	
<ul style="list-style-type: none"> Primary information ID Issuer identification code Set of serial numbers 	

Activity 4.1.7. Store the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> Primary Data Storage receives and stores the set of serial numbers generated <p>Primary Data Storage receives and stores the set of serial numbers generated by the ID Issuer.</p>	<ul style="list-style-type: none"> Primary Data Storage
Inputs	
<ul style="list-style-type: none"> Sequential number issuance request ID 	
Outputs	
<ul style="list-style-type: none"> Set of serial numbers received. 	

4.2. Generate the unique identifiers and incorporate into data carriers – aggregation



Activity 4.2.1. Collect 'secondary information'	
Description	Responsible
<ul style="list-style-type: none"> Collection of the 'secondary information' <p>Manufacturers and importers collect the following secondary information of each unit packet of tobacco produced or imported:</p> <ul style="list-style-type: none"> - Manufacturing timestamp 	<ul style="list-style-type: none"> Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> Production / import information 	
Outputs	
<ul style="list-style-type: none"> Secondary information 	

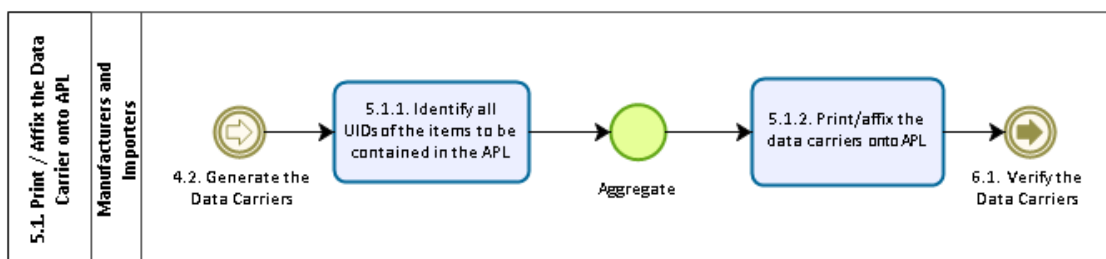
Activity 4.2.2. Consolidate data	
Description	Responsible

<ul style="list-style-type: none"> ▪ Consolidation of the serial number with the primary information When the manufacturers and importers receive the serial number, they consolidate all the information (primary information, ID Issuer identification code, serial number and secondary information), creating a unique identifier for each of the aggregation packaging levels produced in the EU or destined for the EU market. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Primary information ▪ ID Issuer identification code ▪ Serial number ▪ Secondary information 	
Outputs	
<ul style="list-style-type: none"> ▪ UID created for aggregation packaging levels 	

Activity 4.2.3. Generate data carriers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Generation of the data carrier The unique identifier of each aggregation packaging level is transformed into a data carrier. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ UID created for each aggregation packaging level 	
Outputs	
<ul style="list-style-type: none"> ▪ Data carrier for each aggregation packaging level 	

5. Print / affix the data carrier onto the aggregation packaging levels

5.1. Print / affix the data carrier onto aggregation packaging levels (APL)

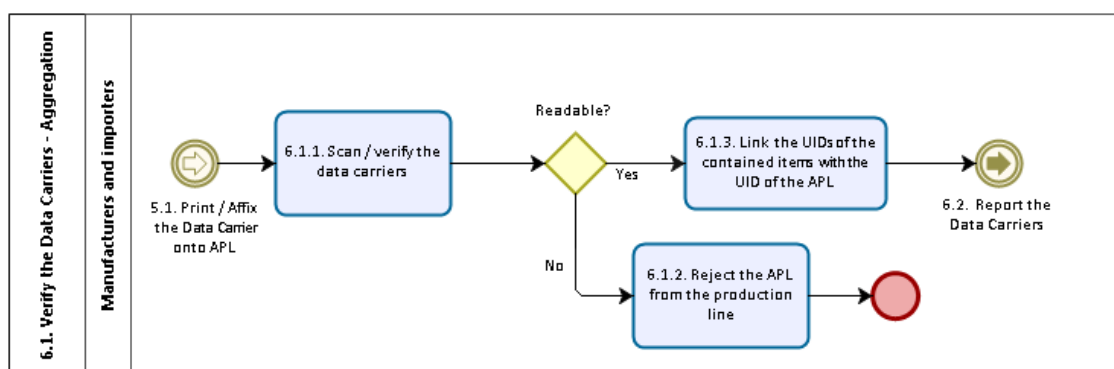


Activity 5.1.1. Identify all unique identifiers of the items to be contained in the APL	
Description	Responsible
<ul style="list-style-type: none"> ▪ Identify all unique identifiers of the items to be contained in the APL Before proceeding with the aggregation itself, the unique identifiers of the items to be contained in the aggregation packaging levels must be identified, in order to create the link with the unique identifier of the APL. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ UIDs of the items to be contained in the APL 	
Outputs	
<ul style="list-style-type: none"> ▪ UIDs of the items to be contained in the APL 	

Activity 5.1.2 Print / affix the data carrier onto aggregation packaging levels	
Description	Responsible
<ul style="list-style-type: none"> ▪ Print / affix the data carrier onto aggregation packaging levels When all necessary data carriers are created, the tobacco manufacturers and importers can start printing/ affixing the data carriers onto the aggregation packaging levels. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Data carriers ▪ Aggregation packaging levels 	
Outputs	
<ul style="list-style-type: none"> ▪ Aggregation packaging levels marked with data carriers 	

6. Data carriers verification and unique identifiers reporting - aggregation packaging levels

6.1. Verify the data carriers – aggregation packaging levels



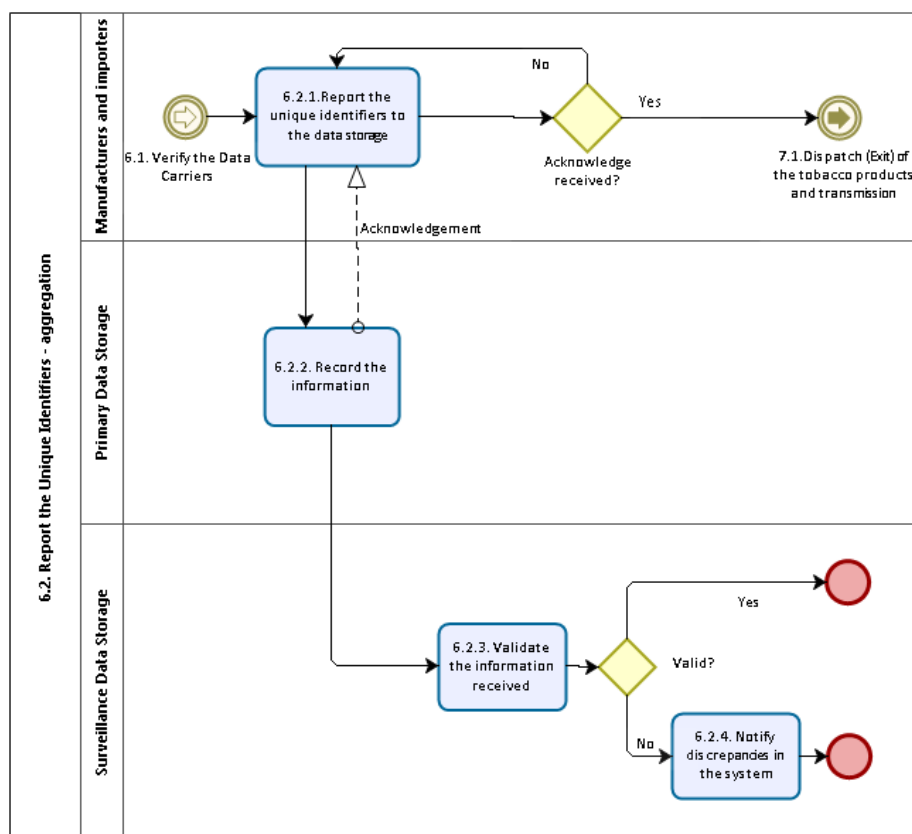
Activity 6.1.1. Scan / verify the data carriers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Scan / verification of the data carriers applied The scanners must scan and read all the aggregation packaging levels produced on the production lines. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Aggregation packaging levels marked with a data carrier 	
Outputs	
<ul style="list-style-type: none"> ▪ Records of the data carriers 	

Activity 6.1.2. Reject unreadable aggregation packaging levels from the production line	
Description	Responsible
<ul style="list-style-type: none"> ▪ Unreadable aggregation packaging levels expelled from the production line If the printed data carrier was unreadable, the aggregation packaging level enters a reverse logistics procedure, in which the tobacco products are repackaged, in order to get a new unique identifier. The process of deactivation of the serial numbers is triggered. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Unreadable aggregation packaging levels 	
Outputs	

- Unreadable aggregation packaging levels expelled from the production line

Activity 6.1.3. Link the UIDs of the contained items with the UID of the APL	
Description	Responsible
<ul style="list-style-type: none"> ▪ Link the UIDs of the contained items with the UID of the APL With the UIDs of the contained items identified and the data carrier of the APL scanned, it is possible to create a link following a parent-child relation between the APL and the items contained in it. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ UIDs of the items contained in the APL; data carrier of the APL 	
Outputs	
<ul style="list-style-type: none"> ▪ Link created between the APL and the items contained within it 	

6.2. Report the unique identifiers – aggregation packaging levels



Activity 6.2.1. Report the unique identifiers to the Primary Data Storage	
Description	Responsible
<ul style="list-style-type: none"> ▪ Communication to the Primary Data Storage of the data carriers scanned: serial numbers used The scanners must transmit to the Primary Data Storage all the data carriers scanned. 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	

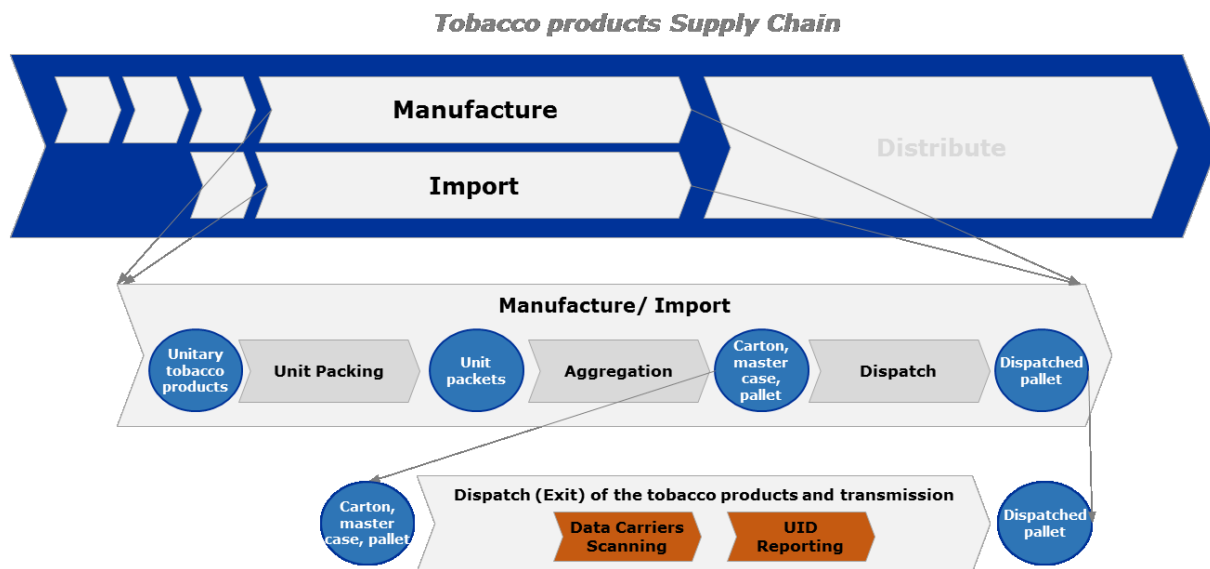
Outputs
▪ N/A

Activity 6.2.2. Record the information	
Description	Responsible
<ul style="list-style-type: none"> ▪ Record the reception information After receiving the report from the manufacturers/importers, the Primary Data Storage records all unique identifiers that were reported and sends an acknowledgment to confirm that the report has been received and understood (the message is sent in the due format and language). The retry policy, described in the Messaging Events section, applies. The information is transmitted to the Surveillance Data Storage. 	<ul style="list-style-type: none"> ▪ Primary Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 6.2.3. Validate the information received	
Description	Responsible
<ul style="list-style-type: none"> ▪ The validation of the information received comprises two stages: <ul style="list-style-type: none"> ▪ Valid UIDs verification (e.g. the UID has not been scanned before nor deactivated, the UID matches the information reported by the ID Issuer at generation, the UID elements are valid, etc.). ▪ Data analytics rules verification (e.g. list of unused serial numbers or UIDs grouped per different criteria, unusual patterns in comparison with other manufacturers or importers, etc.) 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

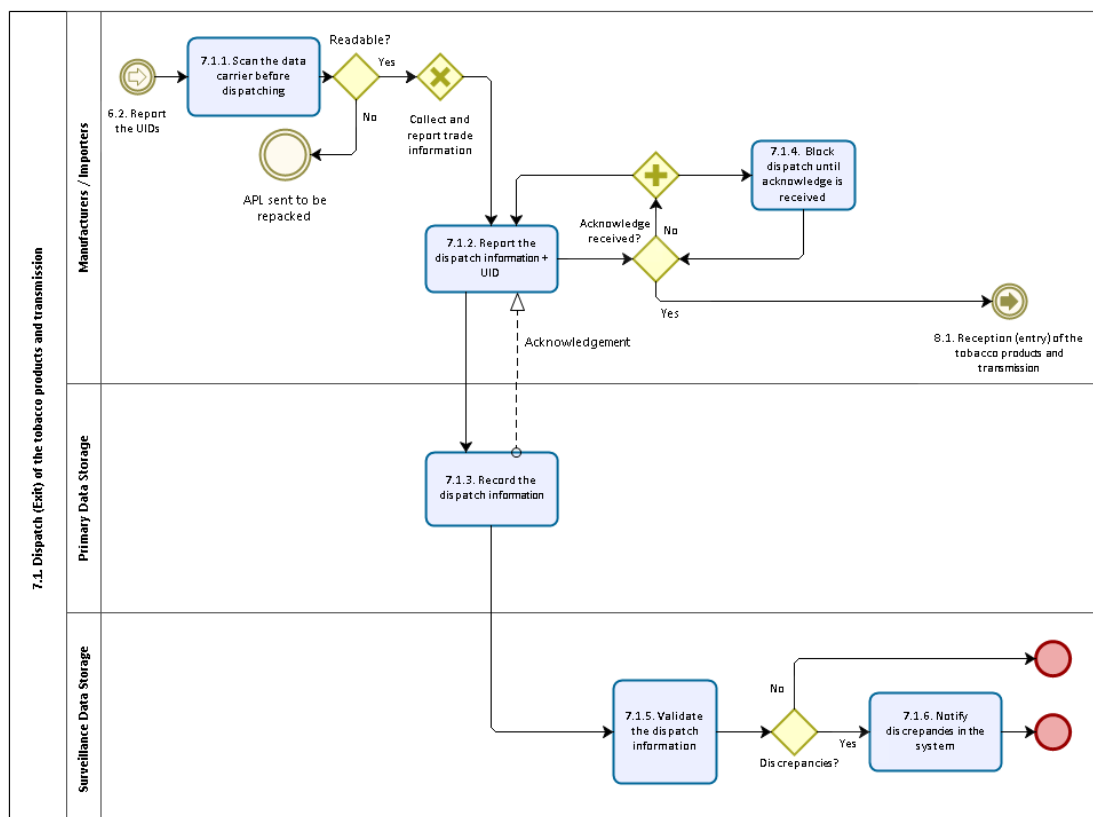
Activity 6.2.4. Notify discrepancies in the system	
Description	Responsible
<ul style="list-style-type: none"> ▪ Notification to the competent authorities if the serial number scanned cannot be found on the list of serial numbers generated (and assigned to a manufacturers/importer) or does not correspond with the serial numbers of the items contained in that aggregation packaging level If the serial number scanned cannot be found on the list of serial numbers generated, a notification is sent by the Surveillance Data Storage in order to take the necessary actions. 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Discrepancies found after the validation of the serial numbers by the Surveillance Data Storage 	
Outputs	
<ul style="list-style-type: none"> ▪ Notification in case of discrepancies 	

1.3.2.4. Dispatch (from manufacturers / importers)



7. Dispatch (exit) of the tobacco products and transmission

7.1. Dispatch (exit) of the tobacco products and transmission



Activity 7.1.1. Scan the data carrier before dispatching

Description	Responsible
-------------	-------------

<ul style="list-style-type: none"> ▪ Scan the data carrier before dispatching <ul style="list-style-type: none"> ▪ Before dispatching the aggregation packaging levels, the manufacturers/wholesalers have to scan the data carriers to generate the last record before the products leave their responsibility. At this moment, manufacturers/wholesalers must guarantee that all data carriers are readable. ▪ If the data carrier is readable, the information is reported to the Data Storage and the pallets are dispatched to the next client, which may be another wholesaler/ distributor. ▪ If the unique identifier is not readable, the aggregation packaging levels are sent to be repackaged. The process of deactivation of the unique identifiers is triggered. 	<ul style="list-style-type: none"> ▪ Manufacturers / importers
Inputs	
<ul style="list-style-type: none"> ▪ Data carriers printed/ affixed onto cartons, master cases or pallets 	
Outputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	

Activity 7.1.2. Report the dispatch information	
Description	Responsible
<ul style="list-style-type: none"> ▪ Report the dispatch information and unique identifier <ul style="list-style-type: none"> ▪ After scanning the tobacco products to read the unique identifier and before dispatching, the manufacturers/importers report the dispatch information to the Primary Data Storage. ▪ This way, the Data Storage can control the last record under the responsibility of the manufacturers/importers. 	<ul style="list-style-type: none"> ▪ Manufacturers / importers
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 7.1.3. Record the dispatch information	
Description	Responsible
<ul style="list-style-type: none"> ▪ Record the dispatch information After receiving the report from the manufacturers/importers, the Primary Data Storage records all unique identifiers and sends an acknowledgement to confirm that the message has been received and understood (the message is sent in the due format and language). The retry policy, described in the Messaging Events section, applies. The information is transmitted to the Surveillance Data Storage. 	<ul style="list-style-type: none"> ▪ Primary Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 7.1.4. Block dispatch until acknowledgement is received	
Description	Responsible
<ul style="list-style-type: none"> ▪ Products shall not be dispatched until an acknowledgement from the Primary Data Storage has been received Manufacturers and importers shall only proceed to dispatch the tobacco products once the Primary Data Storage has sent an acknowledgement confirming that the report information has been received and understood (the message is sent in the due format and language). 	<ul style="list-style-type: none"> ▪ Manufacturers / importers
Inputs	

N/A
Outputs
N/A

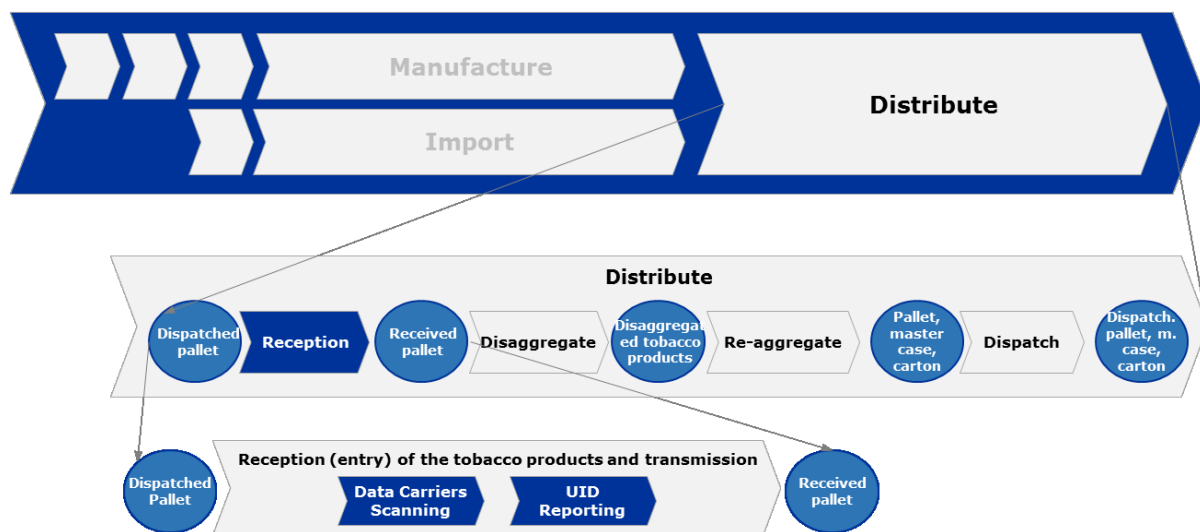
Activity 7.1.5. Validate the dispatch information	
Description	Responsible
<ul style="list-style-type: none"> ▪ The validation of the dispatch information received comprises two stages: <ul style="list-style-type: none"> ▪ Valid UID verification (e.g. the UID has not been scanned before nor deactivated, the UID matches with the information reported by the ID Issuer at the generation, the UID elements are valid, etc.) ▪ Data analytics rules verification (e.g. list of unused serial numbers or UIDs grouped per different criteria, unusual patterns in comparison with other manufacturers or importers, etc.) 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 7.1.6. Notify discrepancies in the system	
Description	Responsible
<ul style="list-style-type: none"> ▪ Notify the discrepancies in the system to the competent authorities <ul style="list-style-type: none"> ▪ If the Surveillance Data Storage finds discrepancies in the system the situation must be communicated. ▪ From the moment of obtaining this information, it is necessary to act accordingly. 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ N/A 	
Outputs	
<ul style="list-style-type: none"> ▪ Notification of the discrepancies found during the control of the unique identifiers reported 	

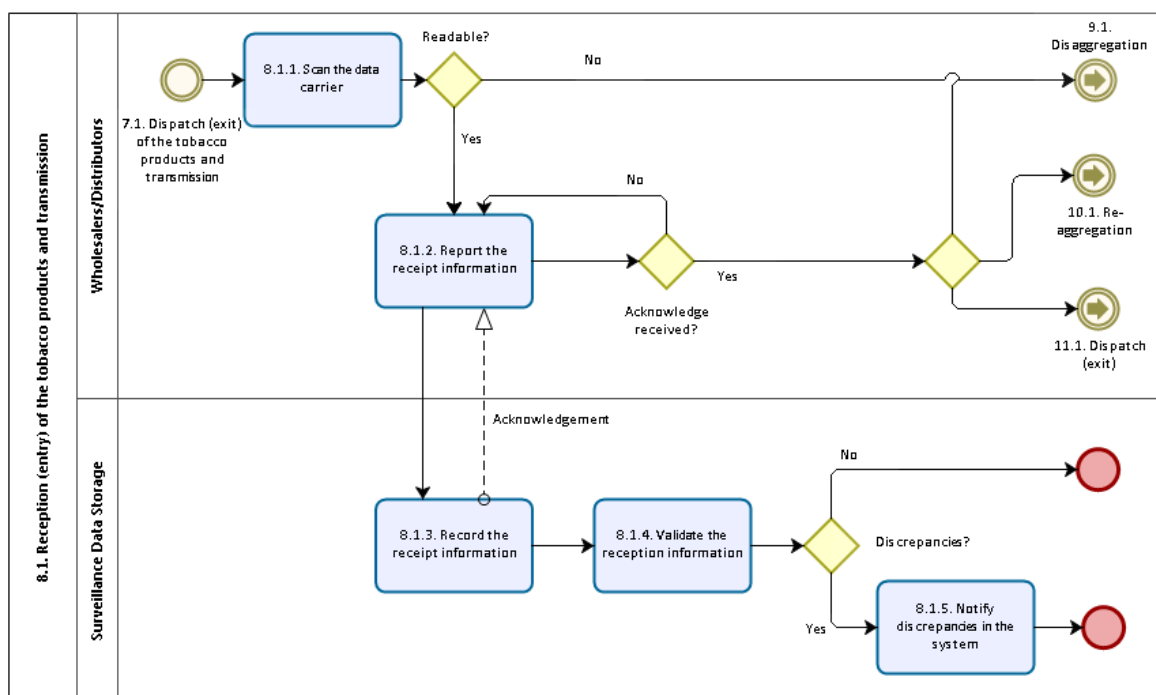
1.3.2.5. Distribution events

8. Reception (entry) of the tobacco products and transmission

Tobacco products Supply Chain



8.1. Reception (entry) of the tobacco products and transmission



Activity 8.1.1. Scan the data carrier

Description	Responsible
<ul style="list-style-type: none"> ▪ Scan the data carrier <ul style="list-style-type: none"> ▪ Upon reception, the wholesalers/ distributors must scan the data carriers, making the link between what was dispatched by the tobacco 	<ul style="list-style-type: none"> ▪ Wholesalers/ distributors

<p>manufacturers (importers) or other wholesalers/ distributors and what is received on their premises.</p> <ul style="list-style-type: none"> ▪ If the data carrier is not readable, the wholesaler/distributor shall disaggregate the aggregation packaging level in order to be able to scan the tobacco products. ▪ If the data carrier is readable, the information is reported to the Surveillance Data Storage. 	
Inputs	
<ul style="list-style-type: none"> ▪ Dispatched aggregation packaging level 	
Outputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	

Activity 8.1.2. Report the reception information

Description	Responsible
<ul style="list-style-type: none"> ▪ Report the reception information After scanning the aggregation packaging levels, the wholesalers/ distributors report the reception information with all data carriers that were verified to the Surveillance Data Storage. 	<ul style="list-style-type: none"> ▪ Wholesalers/ distributors
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 8.1.3. Record the reception information

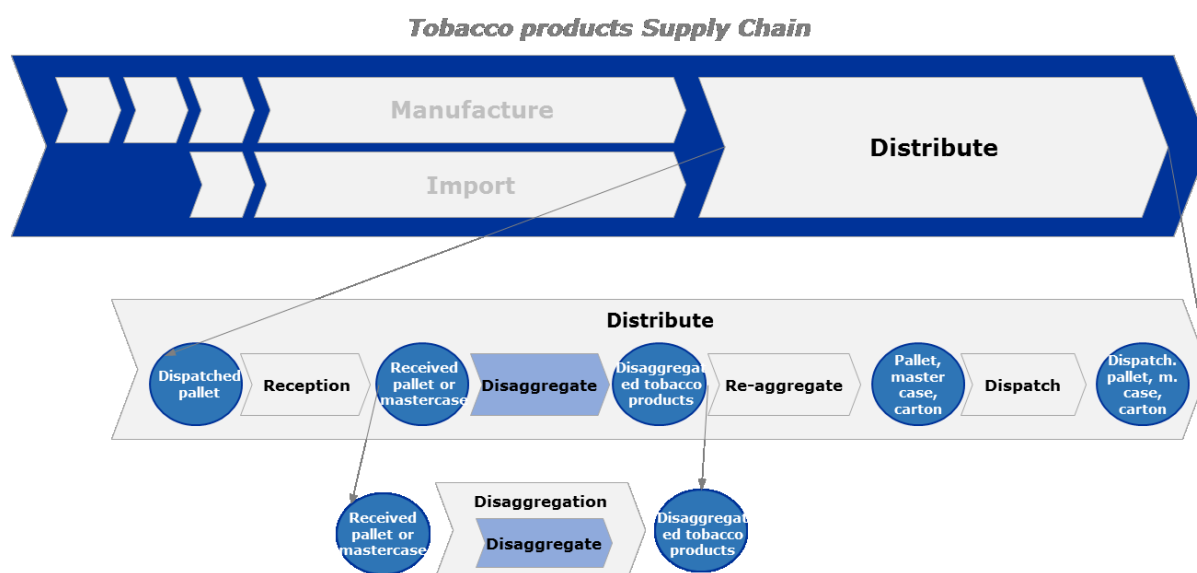
Description	Responsible
<ul style="list-style-type: none"> ▪ Record the reception information After receiving the report from the wholesalers/ distributors, the Surveillance Data Storage records the reception information, with all unique identifiers that were verified. An acknowledgement is sent to the wholesaler/distributor confirming that the reporting message has been received and understood (the message is sent in the due format and language). The retry policy, described in the Messaging Events section, applies. 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 8.1.4. Validate the reception information

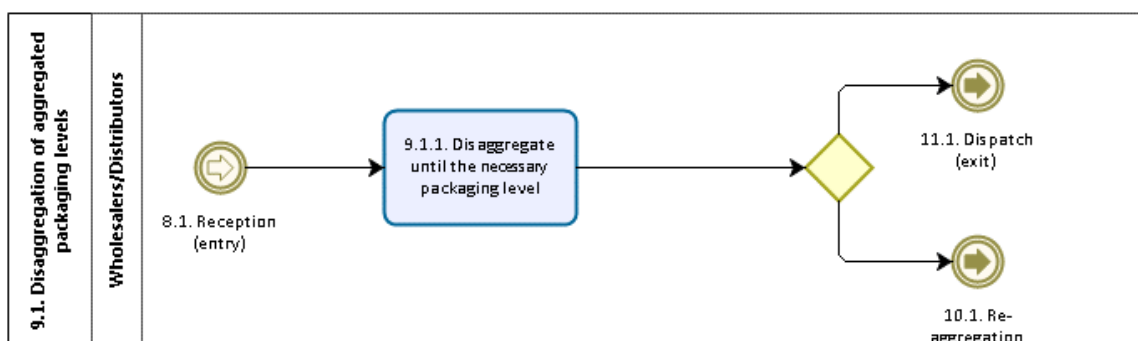
Description	Responsible
<ul style="list-style-type: none"> ▪ The validation of the reception information received comprises two stages: <ul style="list-style-type: none"> ▪ Valid UIDs verification (e.g. the UID has not been scanned before nor deactivated, the UID matches the information reported by the ID Issuer at the generation, the UID elements are valid, etc.). ▪ Data analytics rules verification (e.g. list of unused serial numbers or UIDs grouped per different criteria, unusual patterns in comparison with other manufacturers or importers, etc.). 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 8.1.5. Notify the discrepancies in the system	
Description	Responsible
<ul style="list-style-type: none"> ▪ Notify the discrepancies in the system <ul style="list-style-type: none"> ▪ If the Surveillance Data Storage finds discrepancies in the system, the situation must be communicated. ▪ From the moment of obtaining this information, it is necessary to act accordingly. 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ N/A 	
Outputs	
<ul style="list-style-type: none"> ▪ Notification of the discrepancies found during the control of the unique identifiers reported 	

9. Disaggregation



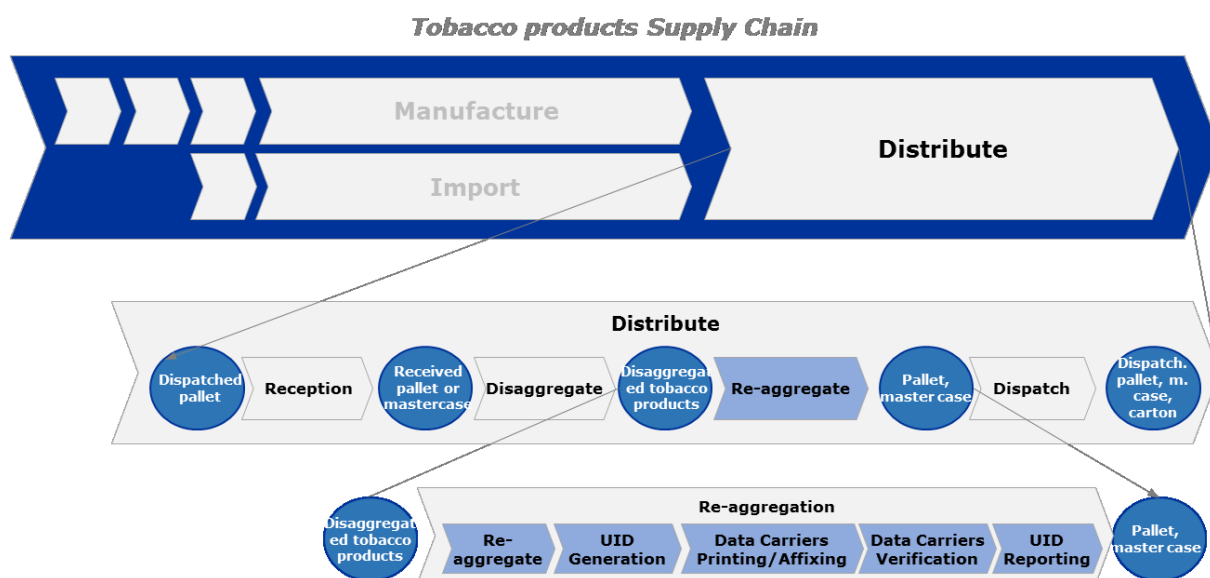
9.1. Disaggregation of aggregation packaging levels



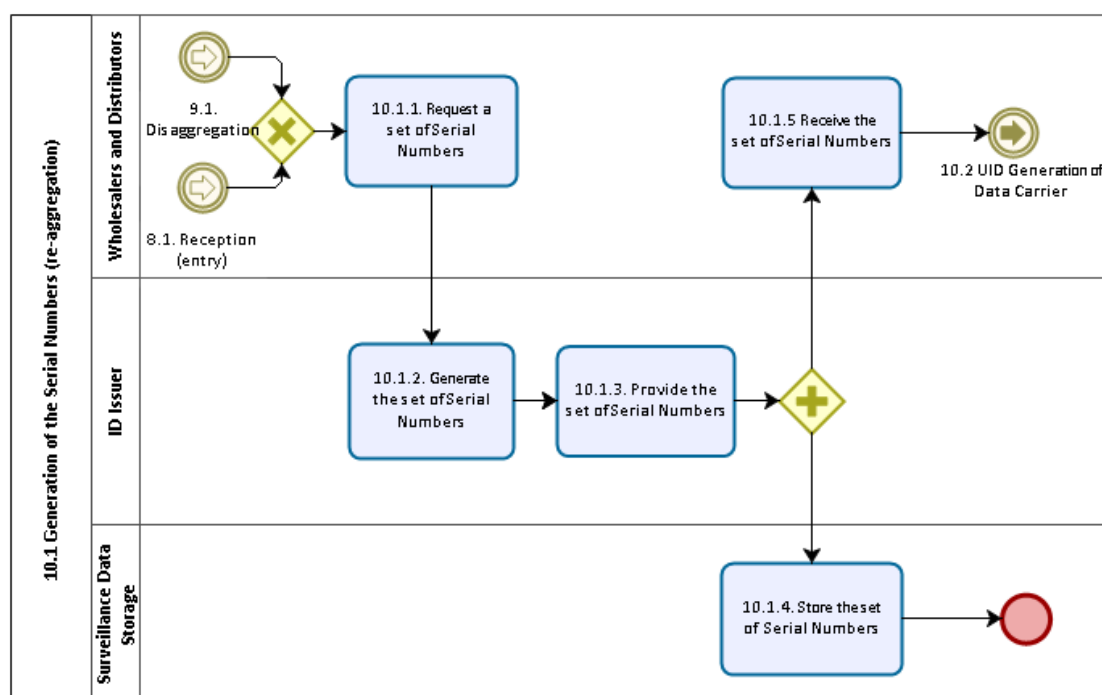
Activity 9.1.1. Disaggregate until the necessary packaging level	
Description	Responsible
<ul style="list-style-type: none"> ▪ Disaggregate until the necessary packaging level The wholesalers / distributors may have the need to disaggregate products (i.e. 	<ul style="list-style-type: none"> ▪ Wholesalers/ distributors

from pallet to master case, and from master case to carton) to meet the orders received.	
Inputs	
▪ Dispatched aggregation packaging levels	
Outputs	
▪ Disaggregation packaging levels	

10. Re-aggregation



10.1. Generation of the serial numbers for the re-aggregation activities



Activity 10.1.1. Request a set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Wholesalers and distributors request a set of serial numbers (communicating primary information) Wholesalers and distributors shall communicate to the ID Issuer the request for the serial numbers they require, providing the primary information: place of re-aggregation. 	<ul style="list-style-type: none"> ▪ Wholesalers/distributors
Inputs	
<ul style="list-style-type: none"> ▪ Primary information 	
Outputs	
<ul style="list-style-type: none"> ▪ Request of serial number with the primary information 	

Activity 10.1.2. Generate the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ▪ ID Issuer generates the set of serial numbers requested for the re-aggregation packaging levels. The ID Issuer generates the serial numbers, according to the standards and rules defined and verifying that the request comes from an authorised (registered in the data server) wholesaler or distributor. 	<ul style="list-style-type: none"> ▪ ID Issuer (under the control of the competent authorities)
Inputs	
<ul style="list-style-type: none"> ▪ Request for serial numbers ▪ Primary information 	
Outputs	
<ul style="list-style-type: none"> ▪ Sequential number issuance request ID 	

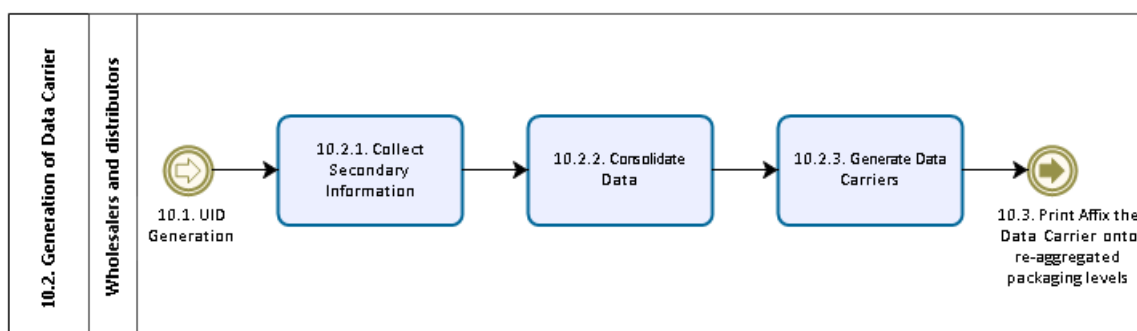
Activity 10.1.3. Provide the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ▪ ID Issuer provides the set of serial numbers to the authorised wholesalers and distributors that requested the serial numbers, and to the Surveillance Data Storage. The ID Issuer generates the serial numbers, according to the standards and rules defined. After the generation, the ID Issuer provides the serial numbers to the wholesalers and distributors, so that they can proceed with marking the re-aggregation levels, and to the Surveillance Data Storage for later validation. 	<ul style="list-style-type: none"> ▪ ID Issuer (under the control of the competent authorities)
Inputs	
<ul style="list-style-type: none"> ▪ Primary information ▪ ID Issuer identification code ▪ Set of serial numbers 	
Outputs	
<ul style="list-style-type: none"> ▪ Set of serial numbers delivered 	

Activity 10.1.4. Store the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Surveillance Data Storage receives and stores the set of serial numbers generated for the re-aggregation packaging levels. Surveillance Data Storage receives and stores the set of serial numbers generated by the ID Issuer for the re-aggregation packaging levels. 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	

<ul style="list-style-type: none"> ▪ Primary information ▪ Set of serial numbers
Outputs
<ul style="list-style-type: none"> ▪ Set of serial numbers stored

Activity 10.1.5. Receive the set of serial numbers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Wholesalers and distributors receive the set of serial numbers requested for the re-aggregation packaging levels <p>Wholesalers and distributors that requested sets of serial numbers for the re-aggregation packaging levels receive them from the ID Issuer.</p>	<ul style="list-style-type: none"> ▪ Wholesalers / distributors
Inputs	
<ul style="list-style-type: none"> ▪ Sequential number issuance request ID 	
Outputs	
<ul style="list-style-type: none"> ▪ Set of serial numbers received 	

10.2. Generation of data carrier for the re-aggregation activities



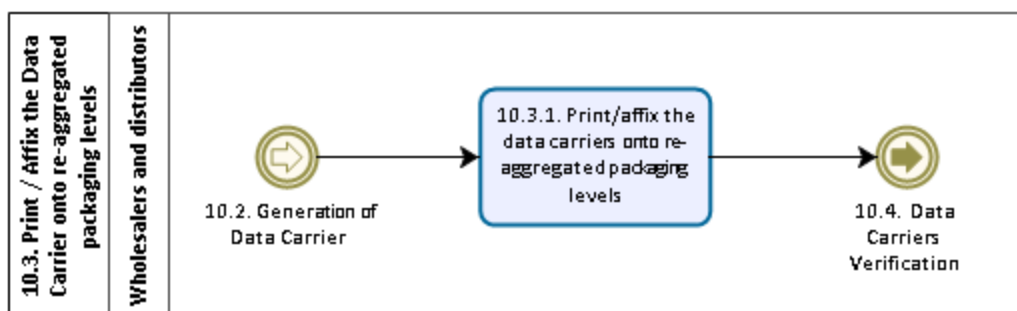
Activity 10.2.1. Collect 'secondary information'	
Description	Responsible
<ul style="list-style-type: none"> ▪ Collection of the 'secondary information' <p>Manufacturers and importers collect the following secondary information of each unit packet of tobacco produced or imported:</p> <ul style="list-style-type: none"> - Manufacturing timestamp 	<ul style="list-style-type: none"> ▪ Manufacturers and importers
Inputs	
<ul style="list-style-type: none"> ▪ Production / import information 	
Outputs	
<ul style="list-style-type: none"> ▪ Secondary information 	

Activity 10.2.2. Consolidate data	
Description	Responsible
<ul style="list-style-type: none"> ▪ Consolidation of the serial number with the primary information by the wholesalers/distributors <p>When the wholesalers/distributors receive the serial number, they consolidate all the information (primary information, ID Issuer identifier, serial number and secondary information), creating a unique identifier for each of the re-</p>	<ul style="list-style-type: none"> ▪ Wholesalers/ distributors

aggregation packing levels.	
Inputs	
<ul style="list-style-type: none"> Primary information Serial number 	
Outputs	
<ul style="list-style-type: none"> Unique identifier created for each re-aggregation packaging level 	

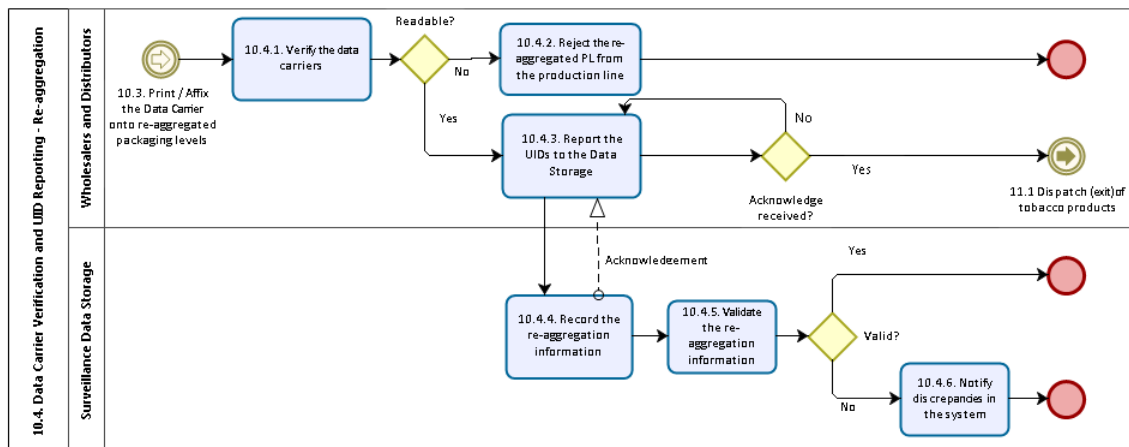
Activity 10.2.3. Generate data carriers	
Description	Responsible
<ul style="list-style-type: none"> Generation of the data carrier The unique identifier of each re-aggregation packaging level is transformed into a data carrier. 	<ul style="list-style-type: none"> Wholesalers/distributors
Inputs	
<ul style="list-style-type: none"> Unique identifier created for each re-aggregation packaging level 	
Outputs	
<ul style="list-style-type: none"> Data carrier for each re-aggregation packaging level 	

10.3. Print / affix the data carrier onto re-aggregation packaging levels



Activity 10.3.1. Print / affix the data carrier onto re-aggregation packaging levels	
Description	Responsible
<ul style="list-style-type: none"> Print / affix the data carrier onto re-aggregation packaging levels When all necessary data carriers are created, wholesalers and distributors can start printing / affixing the data carriers onto the re-aggregation packaging levels. 	<ul style="list-style-type: none"> Wholesalers/distributor
Inputs	
<ul style="list-style-type: none"> Data carriers Re-aggregation packaging levels 	
Outputs	
<ul style="list-style-type: none"> Re-aggregation packaging levels marked with data carriers 	

10.4. Data carriers verification and unique identifiers reporting – re-aggregation packing levels



Activity 10.4.1. Scan / verify the data carriers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Scanning / verification of the data carriers applied The scanners must scan and read all the re-aggregation packaging levels produced by the wholesalers and distributors. 	<ul style="list-style-type: none"> ▪ Wholesalers/ distributors
Inputs	
<ul style="list-style-type: none"> ▪ Re-aggregation packaging levels with a data carrier 	
Outputs	
<ul style="list-style-type: none"> ▪ Records of the data carriers 	

Activity 10.4.2. Reject the re-aggregated packaging levels from the production line	
Description	Responsible
<ul style="list-style-type: none"> ▪ Unreadable re-aggregation packaging levels are expelled from the production line If the printed data carrier is unreadable, the re-aggregation packaging level enters a reverse logistics procedure, in which the tobacco products are repackaged, in order to get a new unique identifier. The processes for deactivation of the serial numbers are triggered. 	<ul style="list-style-type: none"> ▪ Wholesalers/ distributors
Inputs	
<ul style="list-style-type: none"> ▪ Unreadable re-aggregated packaging levels 	
Outputs	
<ul style="list-style-type: none"> ▪ Unreadable re-aggregated packaging levels expelled from the production line 	

Activity 10.4.3. Report the unique identifiers to the Surveillance Data Storage	
Description	Responsible
<ul style="list-style-type: none"> ▪ Communication to the Surveillance Data Storage of the data carriers scanned: serial numbers used The scanners must transmit to the Surveillance Data Storage all the data carriers scanned in the re-aggregation packaging levels. 	<ul style="list-style-type: none"> ▪ Wholesalers/ distributors
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 10.4.4. Record the re-aggregation information

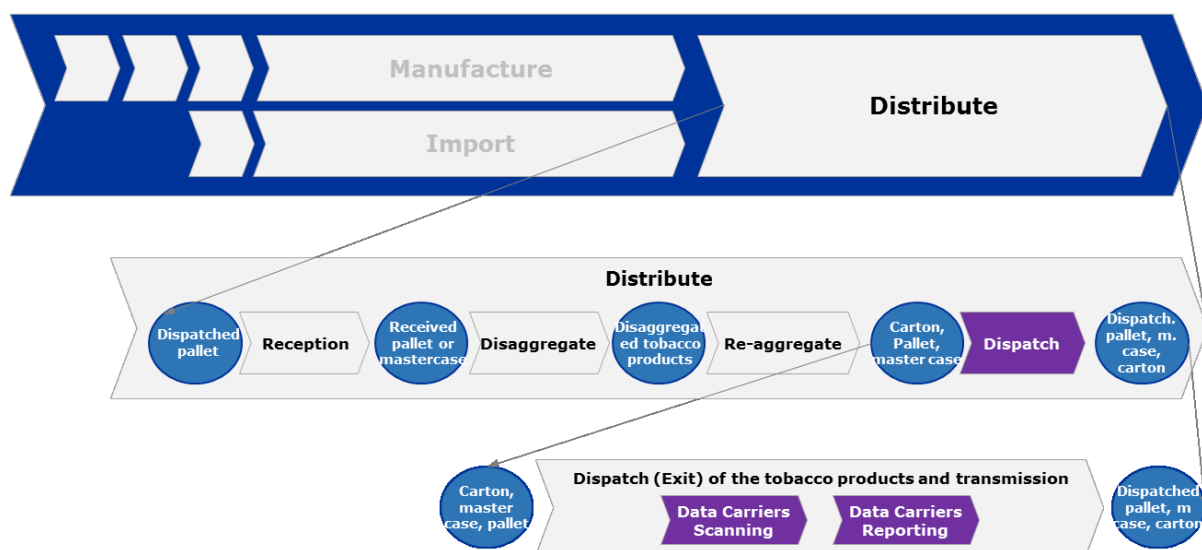
Description	Responsible
<ul style="list-style-type: none"> ▪ Record the re-aggregation information After receiving the report from the wholesalers/ distributors, the Surveillance Data Storage records all information in the unique identifiers. An acknowledgement is sent to the wholesaler/distributor confirming that the reporting message has been received and understood (the message is sent in the due format and language). The retry policy, described in the Messaging Events section, applies. 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 10.4.5. Validate the re-aggregation information	
Description	Responsible
<ul style="list-style-type: none"> ▪ The validation of the information received comprises two stages: <ul style="list-style-type: none"> ▪ Valid UIDs verification (e.g. the UID has not been scanned before nor deactivated, the UID matches the information reported by the ID Issuer at generation, the UID elements are valid, etc.). ▪ Data analytics rules verification (e.g. list of unused serial numbers or UIDs grouped per different criteria, unusual patterns in comparison with other manufacturers or importers, etc.). 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

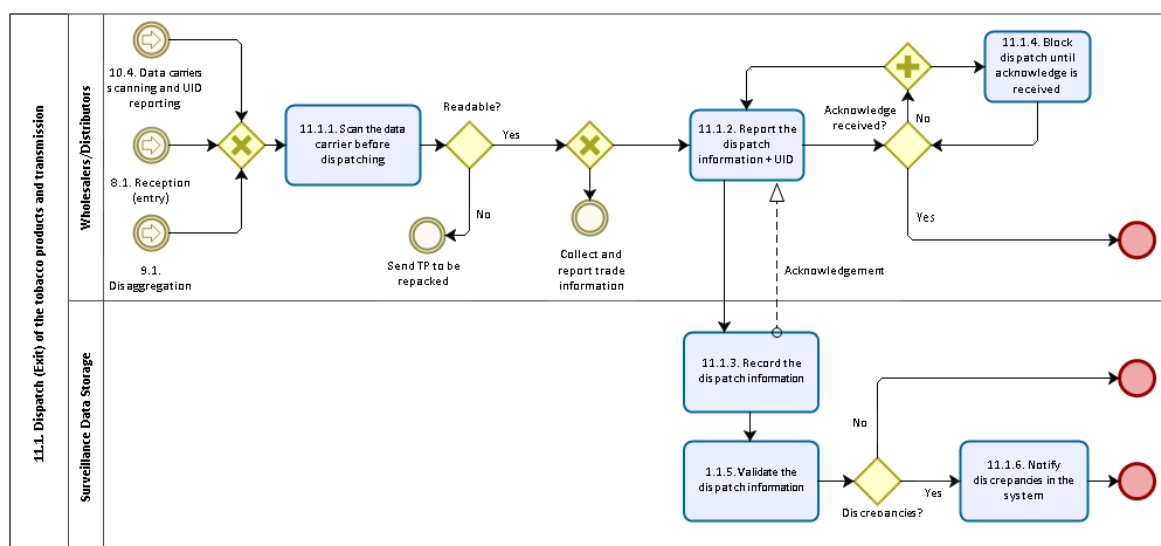
Activity 10.4.6. Notify of discrepancies in the system	
Description	Responsible
<ul style="list-style-type: none"> ▪ Notification to the competent authorities if discrepancies exist between the serial numbers generated (and assigned to a wholesaler/distributor) and the serial numbers scanned If discrepancies are found after the validation of the information contained in the data carriers scanned, a notification is sent by the Surveillance Data Storage to the competent authorities in order to trigger the necessary actions. 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Discrepancies found after the validation of the serial numbers by the Surveillance Data Storage 	
Outputs	
<ul style="list-style-type: none"> ▪ Notification in case of discrepancies 	

11. Dispatch (exit) of the tobacco products and transmission

Tobacco products Supply Chain



11.1 Dispatch (exit) of tobacco products and transmission



Activity 11.1.1. Scan the data carrier before dispatching

Description	Responsible
<ul style="list-style-type: none"> ▪ Scan the data carrier before dispatching <ul style="list-style-type: none"> ▪ Before dispatching, the wholesalers / distributors must scan the data carriers to generate the last record before the products leave their responsibility. At this moment, wholesalers / distributors must guarantee that all data carriers are readable. ▪ If the data carrier is readable, the information is reported to the Surveillance Data Storage, and the pallets are dispatched to the next client, which may be another wholesaler / distributor. ▪ If the data carrier is not readable, the aggregation packaging level or the re-aggregation packaging level is sent to be re-packaged, and the process for deactivation of the serial numbers is triggered. 	<ul style="list-style-type: none"> ▪ Wholesalers/ distributors
Inputs <ul style="list-style-type: none"> ▪ Data carriers printed/ affixed onto cartons, master cases or pallets 	
Outputs	

<ul style="list-style-type: none"> ▪ Unique identifiers
--

Activity 11.1.2. Report the dispatch information and unique identifiers	
Description	Responsible
<ul style="list-style-type: none"> ▪ Report the dispatch information and unique identifiers <ul style="list-style-type: none"> ▪ After scanning the tobacco products to verify the unique identifiers and before dispatching, the wholesalers/ distributors report the dispatch information, with all the unique identifiers that were verified, and the ones that were unreadable, to the Surveillance Data Storage. ▪ This way, the Surveillance Data Storage can control the last record under the responsibility of the wholesalers/ distributors. 	<ul style="list-style-type: none"> ▪ Wholesalers/ distributors
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 11.1.3. Record the dispatch information	
Description	Responsible
<ul style="list-style-type: none"> ▪ Record the reception information After receiving the report from the wholesalers/ distributors, the Surveillance Data Storage records all unique identifiers and sends an acknowledgement to confirm that the message has been received and understood (the message is sent in the due format and language). The retry policy, described in the Messaging Events section, applies. 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

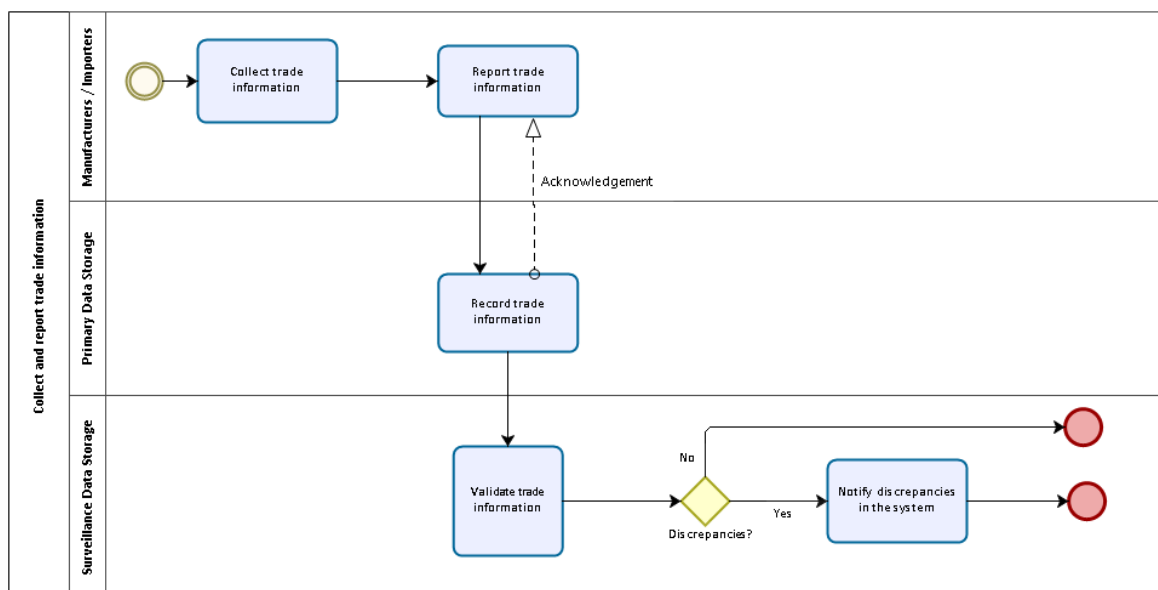
Activity 11.1.4. Block dispatch until acknowledge is received	
Description	Responsible
<ul style="list-style-type: none"> ▪ Products shall not be dispatched until an acknowledgement from the Surveillance Data Storage has been received Wholesalers and distributors shall only proceed to dispatch the tobacco products once the Surveillance Data Storage has sent an acknowledgement confirming that the report information has been received and understood (the message is sent in the due format and language). 	<ul style="list-style-type: none"> ▪ Wholesalers / distributors
Inputs	
N/A	
Outputs	
N/A	

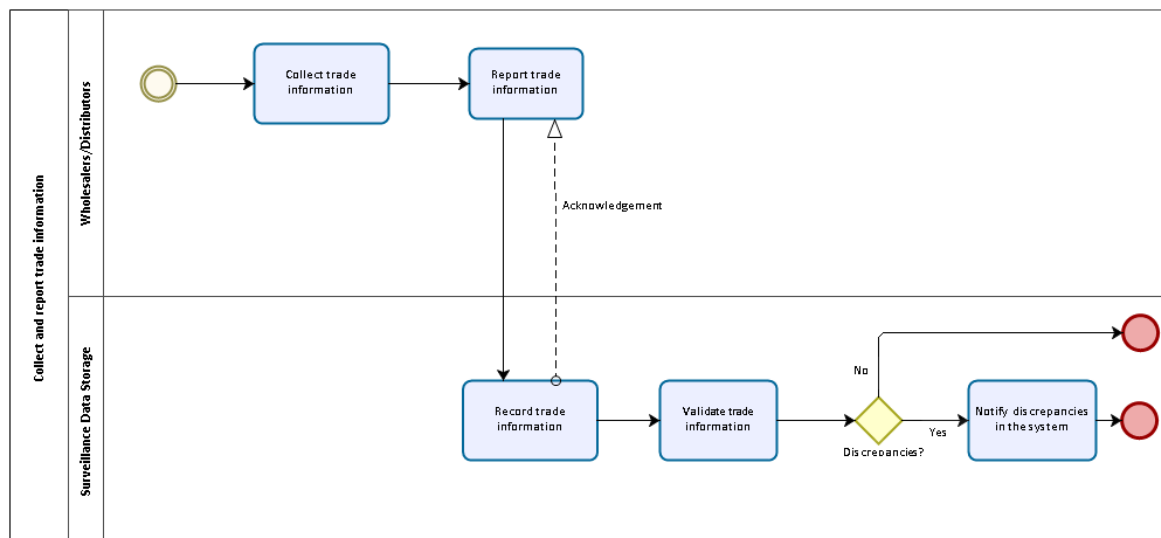
Activity 11.1.5. Validate the dispatch information	
Description	Responsible
<ul style="list-style-type: none"> ▪ The validation of the information received comprises two stages: <ul style="list-style-type: none"> ▪ Valid unique identifiers verification (e.g. the UID has not been scanned before nor deactivated, the UID matches the information reported by the ID Issuer at the generation, the UID elements are valid, etc.). ▪ Data analytics rules verification (e.g. list of unused serial numbers or UIDs grouped per different criteria, unusual patterns in comparison with other 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage

manufacturers or importers, etc.).	
Inputs	
<ul style="list-style-type: none"> ▪ Unique identifiers 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Activity 11.1.6. Notify of discrepancies in the system	
Description	Responsible
<ul style="list-style-type: none"> ▪ Notify of the discrepancies in the system <ul style="list-style-type: none"> ▪ If the Surveillance Data Storage finds discrepancies in the system the situation must be communicated. ▪ From the moment of obtaining this information, it is necessary to act accordingly. 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> ▪ N/A 	
Outputs	
<ul style="list-style-type: none"> ▪ Notification of the discrepancies found during the control of the unique identifiers reported 	

1.3.2.6. Process of collecting and reporting trade information (when dispatching)





Collect trade information	
Description	Responsible
<ul style="list-style-type: none"> ▪ Collect the trade information <ul style="list-style-type: none"> ▪ Once available, the manufacturers/importers or wholesalers/distributors must collect the trade information, as required by the TPD: <ul style="list-style-type: none"> - Invoice(s) - Order number(s) - Payment records 	<ul style="list-style-type: none"> ▪ Manufacturers / importers ▪ Wholesalers / distributors
Inputs	
<ul style="list-style-type: none"> ▪ N/A 	
Outputs	
<ul style="list-style-type: none"> ▪ N/A 	

Report trade information	
Description	Responsible
<ul style="list-style-type: none"> ▪ Report the trade information <ul style="list-style-type: none"> ▪ The manufacturers/ importers or wholesalers/distributors must report the trade information to the Primary Data Storage (for manufacturers and importers) or to the Surveillance Data Storage (for other economic operators). 	<ul style="list-style-type: none"> ▪ Manufacturers / importers ▪ Wholesalers / distributors
Inputs	
<ul style="list-style-type: none"> ▪ N/A 	
Outputs	
<ul style="list-style-type: none"> ▪ Trade information 	

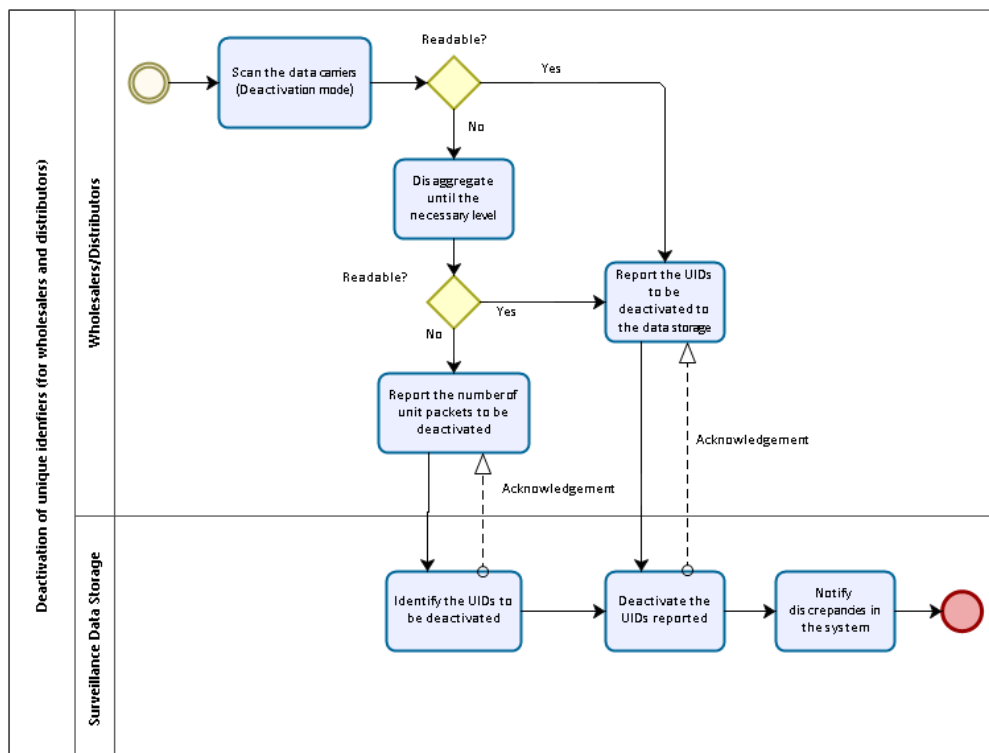
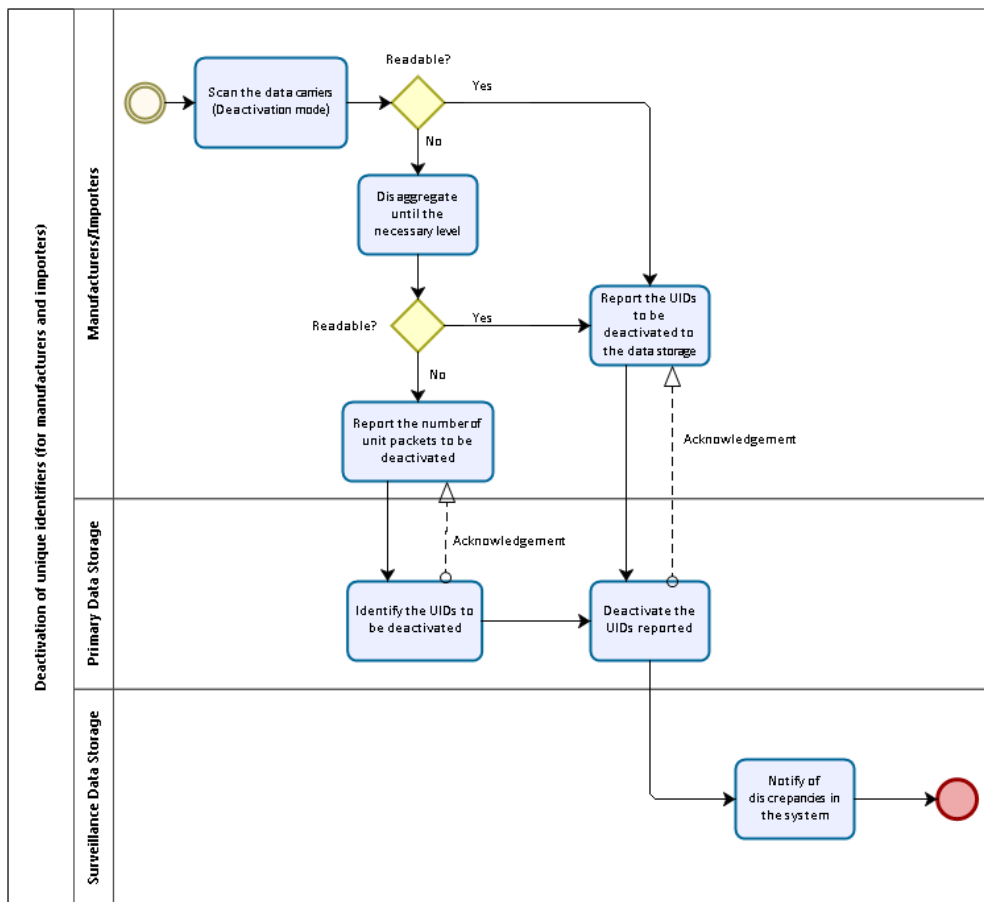
Record trade information	
Description	Responsible
<ul style="list-style-type: none"> ▪ Record the trade information <ul style="list-style-type: none"> ▪ The Primary Data Storage (for dispatch of the manufacturers/ importers) or the Surveillance Data Storage (for dispatch of the wholesalers/distributors) must record the trade information received. 	<ul style="list-style-type: none"> ▪ Primary Data Storage (for manufacturers and importers) ▪ Surveillance Data Storage (for

	wholesalers and distributors)
Inputs	
▪ Trade information	
Outputs	
▪ N/A	

Validate trade information	
Description	Responsible
<ul style="list-style-type: none"> ▪ The validation of the trade information is performed by the Surveillance Data Storage <ul style="list-style-type: none"> ▪ Data analytics and verification rules of the trade information are applied. 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
▪ N/A	
Outputs	
▪ N/A	

Notify of discrepancies in the system	
Description	Responsible
<ul style="list-style-type: none"> ▪ Notification to the system if discrepancies exist with the trade information received <ul style="list-style-type: none"> ▪ If discrepancies are found after the validation of the trade information received, a notification is sent by the Surveillance Data Storage to the competent authorities, triggering the necessary actions. 	<ul style="list-style-type: none"> ▪ Surveillance Data Storage
Inputs	
▪ N/A	
Outputs	
▪ Notification in case of discrepancies	

1.3.2.7. Process of deactivation of unique identifiers



Scan the data carriers (deactivation mode)	
Description	Responsible
<ul style="list-style-type: none"> ▪ Scan the data carriers The scanners (set in deactivation mode) must scan and read all the unit packets to be deactivated. 	<ul style="list-style-type: none"> ▪ Manufacturers/importers ▪ Wholesalers/distributors
Inputs	
<ul style="list-style-type: none"> ▪ Unit packets or aggregation packages to be deactivated 	
Outputs	
<ul style="list-style-type: none"> ▪ Records of the data carriers 	

Disaggregate until the necessary level	
Description	Responsible
<ul style="list-style-type: none"> ▪ Disaggregate until the necessary packaging level The manufacturers/importers and wholesalers/distributors have to disaggregate the products until they reach an aggregation level whose data carrier is readable. 	<ul style="list-style-type: none"> ▪ Manufacturers/importers ▪ Wholesalers/distributors
Inputs	
<ul style="list-style-type: none"> ▪ Aggregation packaging levels 	
Outputs	
<ul style="list-style-type: none"> ▪ Disaggregation packaging levels 	

Report the unique identifiers to be deactivated to the Data Storage	
Description	Responsible
<ul style="list-style-type: none"> ▪ Report the information in the unique identifiers After scanning the packages to verify the unique identifiers, the manufacturers/importers report the information contained in the unique identifiers to the Primary Data Storage and the wholesalers/distributors report it to the Surveillance Data Storage. 	<ul style="list-style-type: none"> ▪ Manufacturers/importers ▪ Wholesalers/distributors
Inputs	
<ul style="list-style-type: none"> ▪ Records of the data carriers 	
Outputs	
<ul style="list-style-type: none"> ▪ Report of the information in the unique identifiers 	

Report the number of unit packets to be deactivated	
Description	Responsible
<ul style="list-style-type: none"> ▪ Report the number of unit packets to be deactivated The manufacturers/importers report the number of unit packets to be deactivated to the Primary Data Storage and the wholesalers/distributors report it to the Surveillance Data Storage. 	<ul style="list-style-type: none"> ▪ Manufacturers/importers ▪ Wholesalers/distributors
Inputs	
<ul style="list-style-type: none"> ▪ N/A 	
Outputs	
<ul style="list-style-type: none"> ▪ Report of the number of unit packets 	

Identify the unique identifiers to be deactivated	
Description	Responsible
<ul style="list-style-type: none"> ▪ Identification of the unique identifiers to be deactivated 	<ul style="list-style-type: none"> ▪ Primary Data Storage (for

Both Data Storages run algorithms to identify the unique identifiers that could not be read based on the records of the database.	<p>manufacturers and importers)</p> <ul style="list-style-type: none"> Surveillance Data Storage (for wholesalers and distributors)
Inputs	
<ul style="list-style-type: none"> Report of the number of unit packets 	
Outputs	
<ul style="list-style-type: none"> Report of the unit packets to be deactivated; acknowledgement of reception of the report. 	

Deactivate the unique identifiers reported	
Description	Responsible
<ul style="list-style-type: none"> Deactivation of the unique identifiers reported <p>Both Data Storages change the status of the unique identifiers from "active" to "deactivated".</p>	<ul style="list-style-type: none"> Primary Data Storage (for manufacturers and importers) Surveillance Data Storage (for wholesalers and distributors)
Inputs	
<ul style="list-style-type: none"> Report of the unit packets to be deactivated 	
Outputs	
<ul style="list-style-type: none"> Report of deactivation activities summary; acknowledgement of reception of the report. 	

Notify of discrepancies in the system	
Description	Responsible
<ul style="list-style-type: none"> Notification to the system if discrepancies exist between the UIDs recorded and the UIDs deactivated <p>If discrepancies are found after the deactivation of the unique identifiers, a notification is sent by the Surveillance Data Storage to the competent authorities, triggering the necessary actions.</p>	<ul style="list-style-type: none"> Surveillance Data Storage
Inputs	
<ul style="list-style-type: none"> Report of deactivation activities summary 	
Outputs	
<ul style="list-style-type: none"> Notification in case of discrepancies 	

1.3.2.8. Recalls of requests, operational and transactional messages

Economic operators also have the possibility to recall requests, operational and transactional messages transmitted to the ID Issuer and the Data Storage(s).

The reasons for recalling the original message may be:

- (1) Reported event did not materialise (only for messages related to dispatch events and trans-loading);
- (2) Message contained erroneous information;
- (3) Other (in which case the reasons must be described).

The recall must include the message recall code provided to the message sender in the acknowledgement of the original message to be recalled and must also contain the following information:

- Reason for recalling the original message
- Description of the reason for recalling the original message (if reason is 'other')
- Any additional explanations for recalling the original message

A recall with respect to operational and logistic events results in flagging the recalled message as cancelled, but does not lead to the deletion of the existing database record.

1.4. System users

1.4.1. RACI matrix

Along with the business processes described in the previous chapter, the responsibility assignment matrix per process, which identifies the roles and responsibilities per actor and activity, is described here.

For this purpose, a RACI matrix is used, in which RACI stands for:

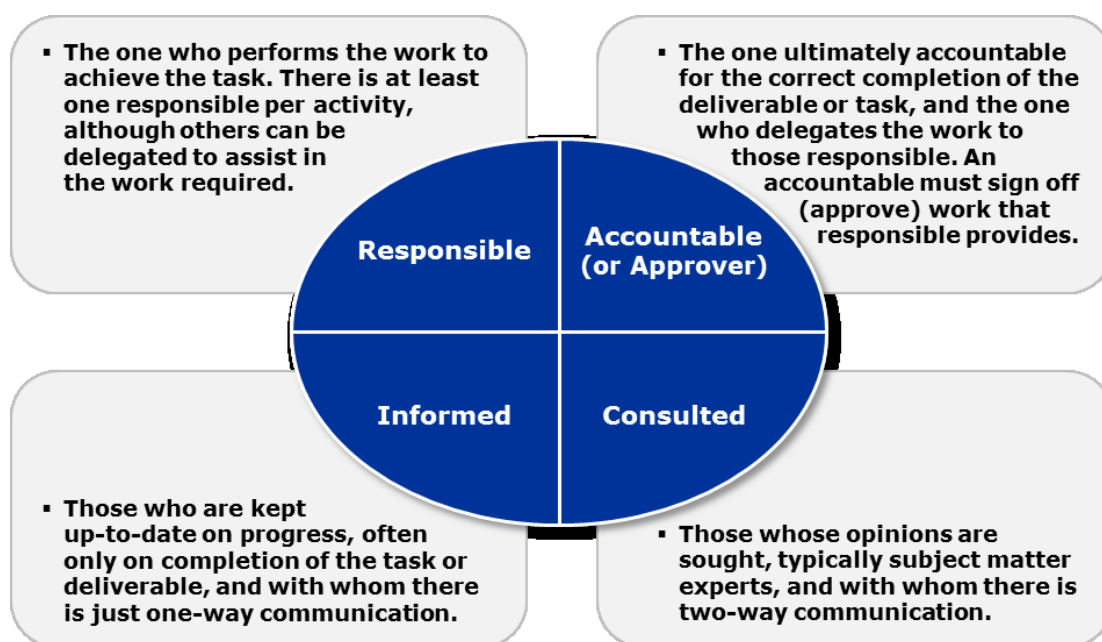


Figure 4: RACI matrix definition

The following users have been identified. Their detailed definition is provided in section 1.4.2:

- Competent Authorities of the Member States
- Tobacco manufacturers and importers of tobacco products
- ID Issuers
- Providers of anti-tampering solutions

- Wholesalers / distributors
- Primary Data Storage Providers
- Surveillance Data Storage Providers

In the table below, the role of each of the system users is specified for each of the **business processes** described in Section 1.3 above. The responsible system users (R) are those who do the work to achieve the task. There is always at least one user responsible for performing a task. Accountables (A) are those that are ultimately answerable for the correct and thorough completion of the deliverable or task, although they may delegate the work to others. Furthermore, some users may be kept informed of the execution of a task. This corresponds to the letter (I).

		Competent Authorities of the Member States	Manufacturers & Importers	ID Issuers	Providers of anti-tampering solutions	Wholesalers & Distributors	Primary Data Storage Providers	Surveillance Data Storage Providers
0. Integration of the Security Features	0.1. Integration of the Security Features	0.1.1. Use the tax stamp as a security feature	R	A				
		0.1.2. Integrate the security feature as part of the production of the packaging material	R	A				
		0.1.3. Integrate the security feature as a label	R	A				
1. Generate UID for Unit Packets	1.1. Generate the serial numbers	1.1.1. Request a set of Serial numbers		R				
		1.1.2. Generate the set of Serial numbers	A		R			
		1.1.3. Provide the set of Serial numbers	A		R			
		1.1.4. Store the set of serial numbers						R
		1.1.5. Receive the set of serial numbers		R				
		1.1.6. Route the set of serial numbers						R
		1.1.7. Store the set of serial numbers					R	
	1.2. Generate the Unique Identifier and incorporate into Data Carriers	1.2.1. Collect 'Secondary Information'		R				
		1.2.2. Consolidate Data		R				
		1.2.3. Generate data carriers		R				

			Competent Authorities of the Member States	Manufacturers & Importers	ID Issuers	Providers of anti-tampering solutions	Wholesalers & Distributors	Primary Data Storage Providers	Surveillance Data Storage Providers	
2. Print/Affix the Data Carriers onto Unit Packets	2.1. Print/Affix the Data Carriers onto Unit Packets	2.1.1. Print / Affix the Data Carrier onto unit packets		R						
3. Data Carrier Verification & UID Reporting	3.1. Verify the Data Carriers	3.1.1. Scan / Verify the Data Carriers		R		I				
		3.1.2. Reject the unit packets from the production line	I	R		I		I	I	
	3.2. Report the UIDs	3.2.1. Report the UIDs to the Data Storage			R		I		I	
		3.2.2. Record the information							R	
		3.2.3. Validate the information received								R
		3.2.4. Notify discrepancies in the system	I							R
4. UID Generation for Aggregation Packaging Levels	4.1. Generate the serial numbers - Aggregation	4.1.1. Request a set of serial numbers		R						
		4.1.2. Generate the set of serial numbers	A		R					
		4.1.3. Provide the set of serial numbers	A		R					
		4.1.4. Store the set of serial numbers							R	
		4.1.5. Receive the set of serial numbers			R					
		4.1.6. Route the set of serial numbers							R	
		4.1.7. Store the set of serial numbers						R		
	4.2. Generate the Data Carriers	4.2.1. Collect 'Secondary Information'			R					
		4.2.2. Consolidate data			R					
		4.2.3. Generate data carriers			R					
5. Data Carrier Printing for aggregation packaging levels	5.1. Print / Affix the Data Carrier onto aggregation packaging levels	5.1.1. Identify all UIDs of the items to be contained in the APL		R						
		5.1.2. Print / Affix the Data Carrier onto aggregation packaging levels		R						
6. Data Carriers Verification & UID Reporting - Aggregation packaging levels	6.1 Verify the Data Carriers	6.1.1. Scan / Verify the Data Carriers		R		I				
		6.1.2. Reject the aggregated packaging levels from the production line	I	R		I		I		
		6.1.3. Link the UIDs of the contained items with the UID of the APL	I	R		I		I		

			Competent Authorities of the Member States	Manufacturers & Importers	ID Issuers	Providers of anti-tampering solutions	Wholesalers & Distributors	Primary Data Storage Providers	Surveillance Data Storage Providers	
	6.2. Report the UIDs	6.2.1. Report the UIDs to the Primary Data Storage		R		I		I		
		6.2.2. Record the information						R		
		6.2.3. Validate the information received							R	
		6.2.4. Notify the competent authorities	I						R	
7. Dispatch (Exit) and transmission	7.1. Dispatch (Exit) of the tobacco products and transmission	7.1.1. Scan the data carrier before dispatching		R						
		7.1.2. Report the dispatch information		R				I		
		7.1.3. Record the dispatch information	I						R	
		7.1.4. Block dispatch until acknowledgement is received		A						
		7.1.5. Validate the dispatch information							R	
		7.1.6. Notify discrepancies in the system	I						R	
8. Reception (Entry) and transmission	8.1. Reception (entry) of the tobacco products and transmission	8.1.1. Scan the data carrier					R			
		8.1.2. Report the receipt information					R		I	
		8.1.3. Record the receipt information	I						R	
		8.1.4. Validate the reception information							R	
		8.1.5. Notify the discrepancies in the system	I						R	
9. Disaggregation	9.1. Disaggregation of aggregated packaging levels	9.1.1. Disaggregate until the necessary packaging level					R			
10. Re-aggregation	10.1. Generation of the serial numbers for the re-aggregation activities	10.1.1. Request a set of serial numbers					R			
		10.1.2. Generate the set of Serial numbers	A		R					
		10.1.3. Provide the set of serial numbers	A		R					
		10.1.4. Store the set of serial numbers							R	
	10.1.5. Receive the set of serial numbers						R			
	10.2. Generation of Data Carrier for the re-aggregation activities	10.2.1. Collect 'Secondary Information'						R		
		10.2.2. Consolidate Data						R		
10.2.3. Generate Data Carriers							R			

			Competent Authorities of the Member States	Manufacturers & Importers	ID Issuers	Providers of anti-tampering solutions	Wholesalers & Distributors	Primary Data Storage Providers	Surveillance Data Storage Providers	
	10.3. Print / Affix the Data Carrier onto re-aggregation packaging levels	10.3.1. Print / Affix the Data Carrier onto re-aggregated packaging levels					R			
	10.4. Data Carriers Verification and UID Reporting	10.4.1. Scan / Verify the Data Carriers					R			
		10.4.2. Reject the unreadable re-aggregated PL from the production line	I				R		I	
		10.4.3. Report the UIDs to the Data Storage					R		I	
		10.4.4. Record the re-aggregation information							R	
		10.4.5. Validate the re-aggregation information							R	
		10.4.6. Notify discrepancies in the system	I						R	
11. Dispatch (Exit) and transmission	11.1. Dispatch (exit) of tobacco products and transmission	11.1.1. Scan the data carrier before dispatching					R			
		11.1.2. Report the dispatch information					R		I	
		11.1.3. Record the dispatch information							R	
		11.1.4. Block dispatch until acknowledge is received					R			
		11.1.5. Validate the dispatch information							R	
		11.1.6. Notify discrepancies in the system	I						R	
Collect and report trade information	Collect and report trade information	Collect trade information	R	R						
		Report trade information	R	R						
		Record trade information						R	R	
		Validate trade information							R	
		Notify discrepancies in the system	I						R	
Deactivate unique identifiers	Deactivate unique identifiers	Scan the data carriers	R	R						
		Disaggregate until the necessary level	R	R						
		Report the UIDs to be deactivated to the data storage	R	R						
		Report the number of unit packets to be deactivated	R	R						
		Identify the UIDs to be deactivated							R	R
		Deactivate UID reported							R	R

			Competent Authorities of the Member States	Manufacturers & Importers	ID Issuers	Providers of anti-tampering solutions	Wholesalers & Distributors	Primary Data Storage Providers	Surveillance Data Storage Providers
		Notify discrepancies in the system	I						R

1.4.2. System user details

The identification of all users that may influence or be impacted by the new Tracking and Tracing System helps to ensure that the needs of all those involved are taken into account. Therefore, understanding the system user details plays an integral role in developing the future design model, and is critical to the success of any interactive system. The system users are described in the chart below, along with each user's role within the system.

Competent authorities of the Member States	
Description of the user type	The competent authorities of the Member States may include the departments, agencies and administrative bodies with responsibility for taxation, customs, health and tobacco control in each of the Member States, including customs or any other enforcement agencies.
Definition	
Accountable for:	The traceability system must be under the control of the competent authorities at all times. It is advisable that the selection of the ID Issuer is carried out by the competent authorities of each of the 28 EU Member States, thereby ensuring that the critical process of generation of the serial numbers is under their control. Each Member State shall select an ID Issuer, or some of them could create clusters to contract jointly an ID Issuer for the sake of efficiency and economies of scale. This may result in the selection of up to 28 ID Issuers.

Tobacco manufacturers and importers of tobacco products	
Description of the user type	'Tobacco manufacturer' is any natural or legal person who manufactures a tobacco product or has a tobacco product designed or manufactured, and markets that product under their name or trademark. 'Importer of tobacco or related products' is the owner of, or a person having the right of disposal over, tobacco or related products that have been brought into the territory of the European Union.
Definition	
Accountable	The tobacco manufacturers and importers of tobacco products are accountable for

for:	<p>requesting the serial numbers (for both the unit packets and the aggregation packaging levels). Once the serial numbers are received, they are accountable for consolidating all the information that is part of the unique identifier, converting it into a data carrier, and applying (print/affix) these data carriers onto the unit packets and the aggregation packaging levels. At unit packet level, they are accountable for the application of the security features.</p> <p>In the process of scanning, they must perform the verification of the codes, and a third party should be asked to install anti-tampering devices in order to introduce necessary checks over this process. They shall also send the unit packets and aggregation packaging levels to be repackaged if the data carrier is unreadable.</p> <p>Before the dispatch (exit) of the tobacco products from their possession, tobacco manufacturers and importers are accountable for scanning the data carriers and reporting the dispatch information to the Primary Data Storage.</p> <p>The manufacturers of tobacco products are also accountable for the integration of the security features on the tobacco products, taking into consideration the different methods that can be used to proceed with this. The security feature may be printed and/or affixed (e.g. using a label). Where it meets the requirements, a Member State may require that its tax stamp be used as the security feature.</p>
------	--

ID Issuer	
Description of the user type	The ID Issuers are independent third parties and are the ones responsible for the generation of the serial numbers, under the mandate and control of the competent authorities.
Definition	
Accountable for:	The ID Issuer can be appointed as responsible, under the control and accountability of the competent authorities of the Member States, for the generation of the serial numbers to be included in the unique identifiers of the unit packets, the aggregation packaging levels and the re-aggregation packaging levels. The serial numbers generated must be sent to the Primary Data Storage (for manufacturers and importers) or to the Surveillance Data Storage (for wholesalers and distributors) as well as to the economic operators that request them.

Providers of anti-tampering solutions	
Description of the user type	<p>'Providers of anti-tampering solutions' are independent third parties that install anti-tampering devices to monitor the verification of the data carriers applied by the manufacturers and importers.</p> <p>The independence of the solution providers must be allowed to be subject to checks by the competent authorities and the information recorded by the devices should be made accessible to them where required.</p>
Definition	
Accountable for:	Monitoring the process of verification of the data carriers applied onto unit packets and the aggregation packaging levels, by means of installing anti-tampering devices.

Wholesalers / distributors

Description of the user type	'Wholesalers and distributors' are all the economic operators involved in the trade of tobacco products, excluding the manufacturers and importers and the retail outlets.
Definition	
Accountable for:	<p>The wholesalers and distributors of tobacco products are accountable for:</p> <ul style="list-style-type: none"> • Scanning the data carriers and reporting the receipt information to the Surveillance Data Storage at the moment of reception (entry) of the tobacco products into their possession. • In the case of re-aggregation, requesting the serial numbers for the re-aggregation packaging levels, creating the unique identifiers and the data carriers, and applying the data carriers onto the re-aggregation packaging levels. • Scanning the data carriers and reporting the receipt information to the Data Storage at the moment of the dispatch (exit) of the tobacco products from their possession.

Primary Data Storage provider(s)

Description of the user type	The Primary Data storage provider(s) has the purpose of hosting data exclusively related to a specific manufacturer or importer. The data storage facility shall be physically located on the territory of the Union. The suitability of the third party, in particular its independence and technical capacities, as well as the contract, shall be approved by the Commission.
Definition	
Accountable for:	<p>(1) The Primary Data Storage provider(s) is accountable for recording the events reported by the manufacturers and importers and transmitting them to the Surveillance Data Storage, which hosts a copy, as specified below:</p> <ul style="list-style-type: none"> • After the scanning/verification of the unique identifiers of the unit packets • After the scanning/verification of the unique identifiers of the aggregation packaging levels • Before the dispatch (exit) of the tobacco products from the facilities of the manufacturers/importers

Surveillance Data Storage provider

Description of the user type	<p>The Surveillance Data storage provider has the purpose of hosting a global copy of all traceability data, including the data stored in each Primary Data Storages. On this basis, the Surveillance Data Storage solution is in a position to offer a comprehensive logical overview of all relevant data, which could be further exploited for the enforcement required by the TPD. Also, this central Surveillance Data Storage solution provides a secure Repository Router component to facilitate the seamless transmission of reports by distributors and wholesalers via a single point.</p> <p>The Data Storage facility shall be physically located on the territory of the Union. The independent third party data storage provider that will establish the Surveillance Data Storage could, e.g. be contracted jointly by the Primary Data Storage providers. The independence and technical capabilities of the surveillance</p>
------------------------------	--

	data storage provider may also be subject to approval by the European Commission.
Definition	
Accountable for:	The Surveillance Data Storage provider is accountable for providing interfaces for data exchange communication, the storing of reported event data and other tracking and tracing data, data validation, reconciliation, and other data treatments furthermore described, such as comparing the information and notifying the competent authorities in case of discrepancies.

1.5. Use cases

Business processes describe the activities of the tobacco products supply chain with a focus on the impact of the Tracking and Tracing System on the activities of the economic operators. However, the System also interacts with other user types, namely: the European Commission, external auditors and the competent authorities. These user types have their own needs and interact with the System differently from the economic operators.

This section provides examples of relevant use cases for the System, which complement the activities and usages addressed in the business processes section. The purpose of these use cases is to help stakeholders refine the System capabilities, describing what each user does and what the System does in response.

It should be noted that the use cases described below are proposed as a starting point and should be further developed.

1.5.1. Audit of data storage

This use case refers to the auditing of both the Primary Data Storage solution and the Surveillance Data Storage solution. The external auditor appointed for monitoring the third party data storage activities of any data storage solution (i.e. Primary or Surveillance) may be different.

1.5.1.1. Actors

- External auditor
- Third party data storage provider
- Primary Data Storage solution
- Surveillance Data Storage solution

1.5.1.2. Preconditions

- The “third party data storage provider” has implemented an Auditing and Monitoring Plan as part of the solution (i.e. Primary Data Storage or Surveillance Data Storage). This plan addresses the following topics, but is not limited to:

- Auditing of vulnerabilities and threats (e.g. default accounts and passwords, easily guessed passwords, missing patches, misconfigurations, excessive privileges, etc.).
- Auditing of data access (e.g. who accessed which entities, when, how and what activities were performed).
- Auditing of database baseline. A database baseline may include the following assets: configuration, schema, users, privileges and structure. This allows deviations from that baseline to be tracked.
- Monitoring of suspicious activities (e.g. abnormal access to sensitive data, unusual behaviour, etc.).
- Monitoring of systems health (e.g. monitoring of software and hardware availability or performance qualities such as throughput).
- Anomalies detection (e.g. monitoring of abnormal functioning).
- Implement server hardening guidelines for securing the system.
- The “third party data storage provider” has provided the “external auditor to the data storage” with credentials and a user manual in order to directly access the storage engine with “full access” privileges while avoiding any mediation component.
- The “third party data storage provider” has provided the “external auditor to the data storage” with credentials and a user manual to access to the data storage query interface.

1.5.1.3. Basic flow

1. Request for auditing evidences. The “external auditor to the data storage” requests **evidences** from the “third party data storage provider”. The evidences include, but are not limited to, the elements listed below:
 - **Potential vulnerabilities and threats** to detect insider or outsider threats and attacks (e.g. default accounts and passwords, weak passwords, missing patches, misconfigurations, excessive privileges, possibility of becoming an administrator, denial of service, buffer overflow, weak or non-existent audit controls, etc.).
 - **Access control policies** (i.e. users, roles and responsibilities) and **management of privileges**.
 - **Accesses** to the Data Storage: 1) who accessed the Data Storage, when and how; 2) what activities were performed in the database by which user type; 3) privileged accesses; 4) accesses to sensitive data; and 5) irregularities in relation to access.
 - **Database baseline** (e.g. configuration, schema, users, privileges and structure).
 - **Monitoring activities**, including: perimeter, anomaly detection (e.g. network, main hardware and software components, etc.), suspicious or unusual access to sensitive data or critical systems.

- **Auditing and monitoring** plan.
 - Certification of **standards compliance** (e.g. ISO/IEC 27001:2014).
2. Delivery of auditing evidences. The “third party data storage provider” prepares and delivers to the “external auditor to the data storage” the evidences that have been requested.
 3. Query tool access for audit purposes. The “external auditor to the data storage” accesses the Data Storage query tool and carries out data checks.
 4. Storage engine access for audit purposes. The “external auditor to the data storage” directly accesses the Data Storage engine and carries out database checks.
 5. Physical access for audit purposes. Optionally, the “external auditor to the data storage” requests physical access to the hosting facilities from the “third party data storage provider”.
 6. Preparation of auditing report. With the information collected through the audit, the “external auditor to the data storage” prepares a report that assesses and monitors the activities of the “third party data storage provider”.
 7. Delivery of auditing report. The “external auditor to the data storage” delivers the audit report to the competent authorities and the Commission.
 8. End of the basic flow.

1.5.2. Notify

This use case refers to the usage of the System as a tool to automatically notify when any condition, logical or temporal, is met.

1.5.2.1. Actors

- Competent authorities
- Commission
- Surveillance Data Storage solution

1.5.2.2. Preconditions

- The Surveillance Data Storage runs a **data analytics** engine that **systematically monitors** all movements relating to unit packets of tobacco products. These movements are reported by all economic operators involved in the tobacco product supply chain, according to the TPD.
- The data analytics engine makes available isolated environments to the competent authorities and the Commission, where the following are configured: a) customised rules or patterns to be detected; and b) notifications to be received when the detection happens.

1.5.2.3. Basic flow

1. Configuration. Each user (i.e. competent authorities and the Commission) is responsible for configuring, on a voluntary basis, his/her own data analytics environment according to their needs and experience on fraud detection, combat of illicit trade and enforcement. The configuration includes, in addition to customised criteria, the notification channel through which the user will be informed when a rule or pattern has been verified or detected.
2. Detection. The data analytics engine of the Surveillance Data Storage systematically monitors all the data evaluating patterns and rules, either when a new event arrives or some temporal condition occurs. When a rule or pattern condition is met, it means that it has been detected.
3. Notification. The user (i.e. competent authority or the Commission) is automatically informed, in near real-time, when one of his/her patterns or rules has been detected.
4. End of the basic flow.

1.5.3. Risk-based surveillance

This use case refers to the usage of the System as a tool for leveraging surveillance activities based on risk-based scenarios.

1.5.3.1. Actors

- Competent authorities
- Commission
- Surveillance Data Storage solution

1.5.3.2. Preconditions

- Adoption of risk-based enforcement. The competent authority follows a risk-based approach for control and enforcement, rather than having officers permanently located at an economic operator's premises.

1.5.3.3. Basic flow

1. Configuration. The competent authority configures his surveillance rules and patterns in the data analytics environment provided by the System (see Notification use case), according to their risk-based scenarios and needs (e.g. detect suspicious activities within the country, combat illicit trade cross-border, etc.).
2. Notification. The competent authority is automatically informed, in near real-time, when a pattern or rule is detected.
3. Make informed decision. The competent authority must decide on the next step:

- a) Retrieve additional data from the Surveillance Data Storage (see Query data use case) in order to gain more insights prior to taking a decision. If necessary, this additional data could be matched with other sources of information such as ECMS, SEED or national systems.
 - b) Request a physical inspection (i.e. planned or immediate).
 - c) At any point of time, it will be possible to recreate the route taken by the product and to determine at what point it was diverted into illicit trade ("tracing").
4. Analyse results. If deemed necessary, the competent authority analyses what has happened and reviews his/her risk-based approach to improve it. This would imply that the competent authority fine-tunes his/her surveillance data analytics accordingly (e.g. changing thresholds or criteria).
 5. End of the basic flow.

1.5.3.4. Alternative flow – Combat of illicit trade

This alternative flow starts at step 1 of the basic flow.

1. Recommended configuration of abnormal or suspicious patterns such as (but not limited to):
 - Detection of **mismatch** between **reception and dispatch** information above a certain threshold.
 - Detection of major **route inconsistencies**, when the intended route differs greatly from the actual route.
 - Detection of intended **market of sale inconsistencies**, when the intended market of sale differs from the actual market.
 - Detection of large volumes of **unused serial numbers**. When a production shift ends, it can be verified how many issued serial numbers have not been used. The rule may be configured to notify above a certain threshold.
 - Detection of large volumes of **abrupt fluctuations/irregularities in trade**. Verification of a certain average of products marked but not dispatched, within a certain period of time, by the importers or manufacturers. Example:
 - ✓ For a certain wholesaler, the measured inflow of products increases exponentially over time in comparison to the outflow of products.
 - Detection of large volumes of **abrupt fluctuations/irregularities in logistics**. Example:
 - ✓ Verification of a certain average of products that the economic operator indicates in the system that have been stolen or lost.
 - Detection of large volumes of product **deviation**, when products dispatched are not received at the expected destination (different from the first retailer) within a certain period of time.

- ✓(All these patterns could apply additional filtering and grouping considerations such as type of products, manufacturers, importers, facilities, or countries involved).

2. End of the alternative flow.
3. Returns to step 2 of the basic flow.

1.5.3.5. Alternative flow – Enforcement

This alternative flow starts at step 1 of the basic flow.

1. Recommended configuration of abnormal or suspicious patterns such as (but not limited to):
 - Detection of large volumes of **delayed reports**, when they are transmitted above the minimum allowed delay (i.e. one hour).
 - Detection of large volumes of products with **incompatible identifiers**, when the System receives reports of items with identifiers not compliant with those prescribed by the System. For example:
 - ✓A unique identifier is scanned in the production facilities and an identical unique identifier (i.e. same serial number) was already reported by one or more other economic operators at other stages in the supply chain, indicating that the unique identifier must already exist.
 - Detection of **lack of reporting** by some economic operators, when the System does not receive some of the events expected, as defined in the business processes (e.g. dispatch, reception, aggregation, etc.)
 - ✓ (All these patterns could apply additional filtering and grouping considerations such as type of products, manufacturers, importers, facilities, or countries involved).
2. End of the alternative flow.
3. Returns to step 2 of the basic flow.

1.5.4. Data access by manufacturers and importers

This use case addresses the manufacturers and importers access to data required in Article 15(8) of the TPD: *"In duly justified cases the Commission or the Member States may grant manufacturers or importers access to the stored data, provided that commercially sensitive information remains adequately protected in conformity with the relevant Union and national law."*

1.5.4.1. Actors

- Manufacturers
- Importers
- Commission

- Competent authorities
- Surveillance Data Storage solution

1.5.4.2. Preconditions

- The manufacturer or importer is previously registered as economic operator participant in the Tracking and Tracing System and his status is valid.
- The manufacturer or importer has interacted with the Surveillance Data Storage related to the recording of movements of unit packets of tobacco products.
- The manufacturer or importer cannot request access to data of unit packets of tobacco products submitted by other manufacturers or importers.

1.5.4.3. Basic flow

1. Information request. The manufacturer or importer requests information of the Surveillance Data Storage from the competent authority. The request must contain the following categories of information:
 - a. Location of manufacturing activities (i.e. FG5Y, GE4W, 3RY5)
 - b. Period of time (i.e. from 2020-01-01 to 2020-04-30)
 - c. Product description (i.e. RD23, GT75)
 - d. Time of manufacturing (i.e. ALL)
 - e. Intended shipment route (i.e. F3, G2, FF, TY)
 - f. Importer (i.e. ALL)
 - g. Reason (i.e. The volume of returns of products RD23 and GT75 is significantly higher in the provided period of time)
2. Evaluation of information request. The competent authority concerned evaluates the request for information and decides on the next step:
 - a. Retrieve all the requested data from the Surveillance Data Storage and deliver it to the manufacturer or importer; or
 - b. Dismiss the information request to the data.
3. End of the basic flow.

1.5.5. Query data

This section lists potential use cases to query data from the System. The uses cases always start when the competent authority requires to access data of tobacco products throughout the supply chain.

1.5.5.1. Actors

- Commission

- Competent authorities
- Surveillance Data Storage solution

1.5.5.2. Preconditions

- The Surveillance Data Storage contains a centralised copy of **all data** of tobacco products movements. These movements are reported by all economic operators involved in the supply chain of tobacco products, in accordance with the TPD.
- The competent authority has the required authorised access to the system.
- The system authenticates the competent authority and authorises access to the query interface.

1.5.5.3. Basic flow

1. The competent authority needs to access data related to tobacco products throughout the supply chain.
2. The competent authority accesses the data query interface.
3. The competent authority commands the data query execution to the system.
4. The System processes the query execution command.
5. The System returns the requested data to the competent authority.
6. End of the basic flow.

1.5.5.4. Alternative flow – query unique identifier

This alternative flow starts at step 3 of the basic flow.

1. The competent authority needs to obtain information concerning a given unique identifier of tobacco products. Examples:
 - a) A Member State would like to retrieve all information concerning a product bearing unique identifier x-y-z (date and place of manufacturing, manufacturing facility, time of manufacture, past location(s), etc.).
 - b) A national investigator would like to retrieve information relating only to the 'current location' of the product bearing unique identifier x-y-z.
2. The competent authority passes the criteria to query data to the System.
3. The System queries the Surveillance Data Storage to extract the data.
4. The System returns to the competent authority the data related to the given criteria such as:
 - a) When the unique identifier is assigned to a unit packet:
 - i. Date of manufacturing
 - ii. Place of manufacturing
 - iii. Manufacturing facility

- iv. Machine used to manufacture the tobacco product
- v. Production shift
- vi. Product description
- vii. Intended market of retail sale
- viii. Intended shipment route
- ix. When applicable, the importer into the Union
- b) When the unique identifier is assigned to an aggregation:
 - i. Date of the aggregation
 - ii. Location of the aggregation
- c) The upper level aggregation
- 5. End of the alternative flow.

1.5.5.5. Alternative flow – query general statistics

This alternative flow starts at step 3 of the basic flow.

1. The competent authority needs to retrieve general statistics (e.g. stocks, inflows/outflows, routes) associated with a particular attribute of the unique identifier (e.g. place of manufacturing, manufacturing facility, machine, intended market of retail etc.). Examples:
 - a) A Member State would like to retrieve the volume of all products that were manufactured in "facility X" in "Trier, Germany" on the date of "01.07.2019".
 - b) A Member State would like to retrieve information on the total volume of product A and product B that left facility X in the period of 01.07.2019 to 31.07.2019.
 - c) A Member State would like to retrieve statistics for the period of 01.07.-31.07.2019 on the volume of unique identifiers (at unit packet level) related to products for which the intended market of retail sale is "the Netherlands".
 - d) A Member State would like to retrieve information on products bearing a unique identifier based on a given number plate of a vehicle transporting tobacco products.
 - e) A Member State would like to retrieve production statistics for the machine with registration number 0123456789. The statistics shall be shown for the period of 01.07.2019 to 31.07.2019.
2. The competent authority passes to the System the criteria to query data.
3. The System queries the Surveillance Data Storage to extract the data.
4. The System returns to the competent authority the data related to the given criteria such as:
 - a) Statistics parameter

- b) Calculation result
 - c) Unique identifier
 - d) Date of manufacturing
 - e) Place of manufacturing
 - f) Manufacturing facility
 - g) Machine used to manufacture the tobacco product
 - h) Intended market of retail sale
5. End of the alternative flow.

1.5.5.6. Alternative flow – comparison and cross-checking of multiple unique identifiers

This alternative flow starts at step 3 of the basic flow.

1. The competent authority needs to compare and crosscheck multiple unique identifiers and the information that they contain. Examples:
 - a) A Member State would like to compare the actual information related to several unique identifiers; for example, to compare the shipment routes of different products (with the same point of departure and shipment destination).
 - b) Based on an automatic comparison, a Member State would like to retrieve a list of all unique identifiers for which the intended and actual shipment destinations are not the same.
2. The competent authority passes to the System the criteria to query data.
3. The System queries the Surveillance Data Storage to extract the data.
4. The System returns to the competent authority the data related to the given criteria, such as:
 - a) Date of manufacturing
 - b) Place of manufacturing
 - c) Manufacturing facility
 - d) Machine used to manufacture the tobacco product
 - e) Production shift
 - f) Product description
 - g) Intended market of retail sale
 - h) Intended shipment route
 - i) When applicable, the importer into the Union
5. End of the alternative flow.

1.5.5.7. Alternative flow – query unique identifier movements

This alternative flow starts at step 3 of the basic flow.

1. The competent authority needs to access data related to movements of unique identifiers of tobacco products.
2. The competent authority passes to the System the criteria to query data.
3. The System queries the Surveillance Data Storage to extract the data.
4. The System returns to the competent authority the data related to the given criteria, such as:
 - a) Activation event details
 - b) Aggregation level events details
 - c) Dispatch events details, including trade data
 - d) Reception events details, including trade data
 - e) Deactivation event details
5. End of the alternative flow.

1.5.5.8. Alternative flow – query aggregations

This alternative flow starts at step 3 of the basic flow.

1. In the case of a unique identifier placed at aggregation level, the competent authority needs to identify all unique identifiers contained therein. Example:
 - a) Unique identifier A-B-C is placed on a carton (aggregation level). The carton contains a number of unit packets each carrying a unique identifier (a-b-c-1, a-b-c-2, a-b-c-3, etc.). A Member State would like to retrieve a list of all unique identifiers connected to the unique identifier A-B-C.
2. The competent authority passes to the System the criteria to query data.
3. The System queries the Surveillance Data Storage to extract the data.
4. The System returns to the competent authority the data related to the given criteria, such as:
 - a) The content of the aggregation
 - b) The upper level aggregations
5. End of the alternative flow.

1.5.5.9. Alternative flow – issuance of serial numbers for economic operators

This alternative flow starts at step 3 of the basic flow.

1. The competent authority needs to access data related to the issuance of serial numbers.
2. The competent authority passes to the System the economic operators to query data.

3. The competent authority passes to the System the period to query data.
4. The System queries the Surveillance Data Storage to extract the data related to the issuance of serial numbers to economic operators for the given period.
5. The System returns to the competent authority the data related to the given criteria, such as:
 - a) Quantity of requested serial numbers within the given period
 - b) Quantity of generated serial numbers within the given period
 - c) Quantity of activated serial numbers
 - d) Quantity of non-activated serial numbers
6. End of the alternative flow.

1.5.5.10. Alternative flow – query serial numbers

This alternative flow starts at step 3 of the basic flow.

1. The competent authority needs to access data related to serial numbers.
2. The competent authority passes to the System the unique identifiers of the serial numbers to query data.
3. The System queries the Surveillance Data Storage to extract the data related to the serial numbers.
4. The System returns to the competent authority the data related to the given serial numbers, such as:
 - a) Serial number issuance requestor economic operator
 - b) Date of the request of the serial numbers issuance
 - c) Date of the generation of the serial numbers
 - d) Date of the delivery of the serial numbers to the economic operator
 - e) Quantity of the requested issuance of the respective generation batch
 - f) Quantity of the generated serial numbers for the batch
5. End of the alternative flow.

1.5.5.11. Alternative flow – query lookup tables

This alternative flow starts at step 3 of the basic flow.

1. The competent authority needs to obtain the lookup tables to further use in an external system.
2. The System queries the Surveillance Data Storage to extract the lookup tables.
3. The System returns to the competent authority the lookup tables data.
4. End of the alternative flow.

1.5.5.12. Alternative flow – any query

This alternative flow starts at step 3 of the basic flow.

1. The competent authority needs to obtain information that has not been considered in the alternative flows above.
2. The competent authority passes to the System the criteria to query data. This criteria could be related to any entity and any field member, even if it is included as a complex attribute within the field (e.g. inner field of a complex XML content), of the Tracking and Tracing System.
3. The System queries the Surveillance Data Storage to extract the data. The storage engine shall be able to support the execution of any query that refers to entities of the System.
4. The System returns to the competent authority the data related to the given criteria.
5. End of the alternative flow.

1.6. Control mechanisms

In order to ensure the correct functioning of the Tracing and Tracking System throughout the supply chain, a number of controls should be implemented. It is important to highlight that the responsibility of implementing these controls should lie primarily with Member States and the Commission but should also extend to independent third parties involved in the establishment and operation of the system. Furthermore, it will be for economic operators to control that their legal obligations are fully met.

The aim of this recommended control mechanism is to ensure that the solution is continuously implemented, supported and maintained according to the standards defined, avoiding deviations that could undermine the full effectiveness of the system.

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
0.1. Integration of the Security Features	Evidence that the security features have been copied by unauthorised parties (i.e. smugglers).	Rotation rules application	Control of the integrity of the container of tobacco products and the presence of the security features
	Security feature not able to be authenticated.	Existence of security features that can be authenticated by the public authorities.	Security features authentication
	Production of security features not secure.	Production should take place in a secure, controlled environment with appropriate security measures in place to protect the premises against unauthorised access.	Establishing controls for full accountability over the security materials used in the production of the security features
	Security features not secure during the transport.	Transport should take place in a secure, controlled environment with appropriate security measures in place to protect the premises against unauthorised access.	Establishing audits to control the transport of the security features
	Security features storage not secure.	Storage should take place in a secure, controlled environment with appropriate security measures in place to protect the premises against unauthorised	Establishing audits of storage

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
		access.	
1.1. Generate the Serial Numbers	Unauthorised parties request serial numbers and/or have access to serial numbers.	Only pre-authorised manufacturers and importers shall be allowed to request serial numbers, avoiding that entities involved in the illicit trade of tobacco products request serial numbers. As the request is sent together with the 'Primary Information', the serial numbers requested are linked to a specific manufacturer or importer.	The user responsible for the management of the registration and authorisation of economic operators shall monitor and control the process of registration of actors and request for serial numbers.
	Connection to the ID Issuer fails and the manufacturers and importers are not able to request serial numbers. Communication failure: problems in the exchange from the manufacturers and importers to the ID Issuer and/or from the ID Issuer to the manufacturers and importers.	Communication redundancy solution shall be applied in order to allow an alternative way to conclude the data exchange.	The infrastructure support area of each party
	Outages of the equipment and tools of the Tracking and Tracing System: the ID Issuer is temporarily unable to generate the serial numbers. Risk of generating duplicates of the serial numbers (ID Issuer provides a serial number and the surveillance system reports that the generated UID already exists).	The generation of the serial numbers is done by an ID Issuer in a secured environment, to avoid risks of manipulation, generation of undesired/unauthorised codes or access by unauthorised parties to the central server. The following controls shall be implemented: <ul style="list-style-type: none"> o Generation should take place in a secure, controlled environment with appropriate security measures in place to protect the central server; and o The algorithms for UID generation must be protected from unauthorised parties, reviewed regularly and updated if needed. 	
	Evidence that the communications between the actors have been intercepted by an unauthorised party.	All the communications channels must be securely encrypted. Authentication of the stakeholders must use state-of-the-art security features.	The data security area of each party; During the audits performed by the competent authorities.
	Unauthorised parties receive the set of serial numbers.	The ID Issuer shall send the serial numbers generated only to the authorised manufacturers and importers that requested the codes.	The system shall be allowed to respond to data queries to obtain information from the registry management in order to trace all the requests for serial numbers received and answered.

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
	Misalignment between the serial numbers generated and the unit packets marked.	The Data Storage receives for the first time the serial numbers generated for the unit packets, which are associated to a specific manufacturer or importer. This information will be later validated at the moment of scanning the data carriers.	Economic Operator; Data Storage Solution Provider. During the audits performed by the competent authorities.
1.2. Generate the Data Carriers	Lack of robustness of the unique identifiers.	Each of the unique identifiers created is unique due to its configuration ('primary information' + 'ID Issuer identifier' + 'serial number' + 'secondary information'). Each of the unique identifiers is linked to a specific manufacturer or importer and to a production line and date, contributing to the traceability of each of the unit packets marked. The serial number shall be a numeric or alphanumeric sequence of a maximum 20 characters, generated by a randomisation algorithm.	The configuration of the unique identifiers (serial numbers + ID Issuer identifier + primary information + secondary information) will feed the data exploitation of the products tracing.
2.1. Print/Affix the Data Carriers onto Unit Packets	Misalignment between the serial numbers generated and the unit packets marked, or risk that not all the unit packets produced (or imported) are marked with a unique identifier. Outages of the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to print/affix the data carriers.	Tobacco manufacturers and importers are obliged to install equipment to count output, as well as devices to control, register, record and transmit the quantities of unit packs produced.	During the audits, the compliance of the equipment installed in the production lines will be monitored, assessed, audited and approved.
3.1. Verify the Data Carriers	Risk that not all the unit packets produced (or imported) are scanned and reported. Outages of the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the	The industry may perform the scanning/verification of the codes, but independent third parties will be asked to install anti-tampering devices in order to introduce necessary checks over this process: - Supervise the scanning/verification equipment area with tamper detection cameras. - Identify the manipulation of the scanning/verifying equipment through user identification. - Match the number of produced	During the audits, the compliance of the equipment installed in the production lines will be monitored, assessed, audited and approved. The regular and unplanned audits performed will target the correct functioning of the scanners with special attention to the tamper-evidence mechanisms implemented.

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
	equipment used to scan the data carriers.	<p>items with the activity in the scanning/verification equipment by using production counters.</p> <ul style="list-style-type: none"> - Assure that all the electronic equipment used in the anti-tampering solution is active through power controllers. <p>These anti-tampering devices must ensure that the scanners and verification equipment are permanently installed in the production lines and that all the unit packets produced in each of the production lines are scanned.</p> <p>All the production lines must be equipped with this equipment and certified by an independent third party before manufacturers and importers are authorised to request serial numbers.</p>	
3.2. Report the UIDs	<p>Communication failure: problems in the messaging from the manufacturers and importers to the Data Storage.</p> <p>Connection to the Data Storage fails and the scanners are not able to connect to the Data Storage.</p>	<p>The scanners must transmit to the Data Storage the information contained in all the data carriers scanned in the production lines. Only those serial numbers scanned and transmitted to the Data Storage will be activated and considered valid to be used through the supply chain.</p> <p>Communication redundancy solutions shall be applied in order to allow an alternative way to conclude the data exchange.</p>	The infrastructure support area of each party.
	Evidence that the communications between the actors have been intercepted by an unauthorised party.	All the communications channels must be securely encrypted. Authentication of the stakeholders must use state-of-the-art security features.	The data security area of each party; During the audits performed by the competent authorities.
	Validation of the serial numbers generated, the unit packets marked and the total production (or imports).	<p>At this point, the Data Storage proceeds to the verification of the serial numbers generated, used and not used.</p> <p>The serial numbers generated are considered valid if they have been duly scanned by the correct manufacturer or importer within the expiry date of each of the serial numbers.</p> <p>An alert is sent to the competent authorities, informing if there are discrepancies between serial numbers generated and data carriers scanned:</p> <ul style="list-style-type: none"> - Data carriers scanned with wrong serial numbers (not 	During the audits performed by the competent authorities.

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
		generated by the ID Issuer or generated for another date, manufacturer, importer or production line). - Serial numbers generated and not used, which must therefore be considered as not valid for use in the supply chain.	
4.1. Generate the Serial Numbers	Unauthorised parties request serial numbers and/or have access to serial numbers.	Only pre-authorized manufacturers and importers shall be allowed to request serial numbers, avoiding that entities involved in the illicit trade of tobacco products request serial numbers. As the request is sent together with the 'Primary Information', the serial numbers requested are linked to a specific manufacturer or importer.	The user responsible for the management of the registration and authorisation of economic operators shall monitor and control the process of registration of actors and request for serial numbers.
	Outages of the equipment and tools of the Tracking and Tracing System: the ID Issuer is temporarily unable to generate the serial numbers. Risk of generating duplicates of the serial numbers (ID Issuer provides a serial number and the surveillance system reports that the generated UID already exists).	The generation of the serial numbers is done by an ID Issuer in a secured environment, to avoid risks of manipulation, generation of undesired/unauthorised codes or access by unauthorised parties to the central server. The following controls shall be implemented: - Generation should take place in a secure, controlled environment with appropriate security measures in place to protect the central server - The algorithms behind the generation of the codes should be protected from unauthorised parties and updated regularly.	
	Evidence that the communications between the actors have been intercepted by an unauthorised party.	All the communication channels must be securely encrypted. Authentication of the stakeholders must use state-of-the-art security features.	The data security area of each party; During the audits performed by the competent authorities.
	Unauthorised parties receive the set of serial numbers.	The ID Issuer shall send the serial numbers generated only to those authorised manufacturers and importers that requested the codes.	The system shall be allowed to respond to data queries to obtain information from the registry management in order to trace all the requests for serial numbers received and answered.
	Misalignment between the serial numbers generated and the unit packets marked.	The Data Storage receives for the first time the serial numbers generated for the unit packets, which are associated to a specific manufacturer or importer. This information will be later validated at the moment of scanning the data carriers.	Economic Operator; Data Storage Solution Provider. During the audits performed by the competent authorities.

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
4.2. Generate the Data Carriers	Lack of robustness of the unique identifiers.	<p>Each of the unique identifiers created is unique due to its configuration ('primary information' + 'serial number' + 'ID Issuer identifier' + ('secondary information')). Each of the unique identifiers is linked to a specific manufacturer or importer and to a production line and date, contributing to the traceability of each of the unit packets marked.</p> <p>The serial number shall be a numeric or alphanumeric sequence of a maximum 20 characters, generated by a randomisation algorithm.</p>	The configuration of the unique identifiers (serial numbers + primary information + ID Issuer identifier + secondary information) will feed the data exploitation of the product tracing.
5.1. Print / Affix the Data Carrier onto aggregation packaging levels	Misalignment between the serial numbers generated and the unit packets marked, or risk that not all the unit packets produced (or imported) are marked with a unique identifier.	Tobacco manufacturers and importers are obliged to install equipment to count output, as well as devices to control, register, record and transmit the quantities of packs produced.	During the audits, the compliance of the equipment installed in the production lines will be monitored, assessed, audited and approved.
	Outages of the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to print/affix the data carriers.		
6.1. Scan the Data Carriers	Risk that not all the unit packets produced (or imported) are scanned and reported.	<p>The industry may perform the scanning/verification of the codes, but independent third parties will be asked to install anti-tampering devices in order to introduce necessary checks over this process:</p> <ul style="list-style-type: none"> - Supervise the scanning/verification equipment area with tamper detection cameras. - Identify the manipulation of the scanning/verifying equipment through user identification. - Match the number of produced items with the activity in the scanning/verification equipment by using production counters. - Assure that all the electronic equipment used in the anti-tampering solution is active through power controllers. <p>These anti-tampering devices</p>	<p>During the audits, the compliance of the equipment installed in the production lines will be monitored, assessed, audited and approved.</p> <p>The regular and unplanned audits performed will target the correct functioning of the scanners with special attention to the tamper-evidence mechanisms implemented.</p>
	Outages of the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to scan the data carriers.		

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
		<p>must ensure that the scanners and verification equipment are permanently installed in the production lines and that all the unit packets produced in each of the production lines are scanned.</p> <p>All the production lines must be equipped with this equipment and certified by an independent third party before manufacturers and importers are authorised to request serial numbers.</p>	
6.2. Report the UIDs	<p>Communication failure: problems in the messaging from the manufacturers and importers to the Data Storage.</p> <p>Connection to the Data Storage fails and the scanners are not able to connect to the Data Storage.</p>	<p>The scanners must transmit to the Data Storage the information contained in all the data carriers scanned in the production lines. Only those serial numbers scanned and transmitted to the Data Storage will be activated and considered valid to be used through the supply chain.</p> <p>A communication redundancy solution shall be applied in order to allow an alternative way to conclude the data exchange.</p>	The infrastructure support area of each party
	Evidence that the communications between the actors have been intercepted by an unauthorised party.	All the communication channels must be securely encrypted. Authentication of the stakeholders must use state-of-the-art security features.	The data security area of each party; During the audits performed by the competent authorities.
	Validation of the serial numbers generated, the aggregation packaging levels marked and the total production (or imports).	<p>At this point, the Data Storage proceeds to the verification of the serial numbers generated, used and not used. The serial numbers generated are considered valid if they have been duly scanned by the correct manufacturer or importer within the expiry date of each of the serial numbers.</p> <p>An alert is sent to the competent authorities, informing if there are discrepancies between serial numbers generated and data carriers scanned:</p> <ul style="list-style-type: none"> - Data carriers scanned with wrong serial numbers (not generated by the ID Issuer or generated for another date, manufacturer, importer or production line). - Serial numbers generated and not used, which must be therefore considered as not valid for use in the supply 	Economic Operator; Data Storage Solution Provider. During the audits performed by the competent authorities.

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
		chain.	
	Outages of the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to scan the data carriers.	Products will not be allowed to leave the responsibility of the manufacturer/importer until an acknowledgement has been received from the Data Storage, confirming that the reporting message has been received and understood.	
7.1. Dispatch (Exit) of the tobacco products and transmission	Communication failure: problems in the messaging from the manufacturers and importers to the Data Storage. Connection to the Data Storage fails and the scanners are not able to connect to the Data Storage.	The scanners must transmit to the Data Storage the information contained in all the data carriers scanned in the production lines. Only those serial numbers scanned and transmitted to the Data Storage will be activated and considered as valid to be used through the supply chain. A communication redundancy solution shall be applied in order to allow an alternative way to conclude the data exchange.	The infrastructure support area of each party.
	Evidence that the communications between the actors have been intercepted by an unauthorised party.	All the communication channels must be securely encrypted. Authentication of the stakeholders must use state-of-the-art security features.	The data security area of each party; During the audits performed by the competent authorities.
	Validation that the traceability information reported is correct (IN-OUT principle).	The Data Storage keeps records of the exit of the tobacco products from the possession of the importers and manufacturers, together with all other relevant dispatch information.	Economic operator; Data Storage Solution Provider. During the audits performed by the competent authorities.
		The Data Storage proceeds to the validation of the dispatch information.	
In case of discrepancies between the dispatch information and other data stored previously, the Data Storage notifies the competent authorities.			

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
8.1. Reception (entry) of the tobacco products and transmission	<p>Communication failure: problems in the messaging from the wholesalers and distributors to the Data Storage.</p> <p>Connection to the Data Storage fails and the scanners are not able to connect to the Data Storage.</p>	<p>Within the specified permitted delay of the entry of the tobacco products into their possession, wholesalers and distributors shall report this movement to the Data Storage.</p> <p>All the communication channels must be securely encrypted. A communication redundancy solution shall be applied in order to allow an alternative way to conclude the data exchange.</p>	<p>The infrastructure support area of each party.</p>
	<p>Evidence that the communications between the actors have been intercepted by an unauthorised party.</p>	<p>All the communication channels must be securely encrypted. Authentication of the stakeholders must use state-of-the-art security features.</p>	<p>The data security area of each party; During the audits performed by the competent authorities.</p>
	<p>Validation that the traceability information reported is correct (IN-OUT principle).</p>	<p>The Data Storage keeps records of the entry of the tobacco product into the possession of the wholesalers and distributors, together with all other relevant reception information.</p>	<p>Economic operator; Data Storage Solution Provider. During the audits performed by the Competent Authorities.</p>
	<p>Validation that the traceability information reported is correct (IN-OUT principle).</p>	<p>The Data Storage proceeds to the validation of the reception information.</p>	
<p>In case of discrepancies between the reception information and other data stored previously, the Data Storage notifies the competent authorities.</p> <p>The Data Storage proceeds to the validation of the disaggregation information.</p> <p>In case of discrepancies between the disaggregation information and other data stored previously, the Data Storage notifies the competent authorities.</p>			
10.1. Generation of the serial numbers for the re-aggregation activities	<p>Unauthorised parties request serial numbers and/or have access to serial numbers.</p>	<p>Only pre-authorised wholesalers and distributors shall be allowed to request serial numbers, avoiding that entities involved in the illicit trade of tobacco products request serial numbers.</p> <p>As the request is sent together with the primary information, the serial numbers requested are linked to a specific wholesaler and distributor.</p>	<p>The user responsible for the management of the registration and authorisation of economic operators shall monitor and control the process of registration of actors and request for serial numbers.</p>

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
	<p>Outages on the equipment and tools of the Tracking and Tracing System: the ID Issuer is temporarily unable to generate the serial numbers.</p> <p>Risk of generating duplicates of the serial numbers (ID Issuer provides a serial number and the surveillance system reports that the generated UID already exists).</p>	<p>The generation of the serial numbers is done by an ID Issuer in a secured environment, to avoid risks of manipulation, generation of undesired/unauthorised codes or access by unauthorised parties to the central server. The following controls shall be implemented:</p> <ul style="list-style-type: none"> o Generation should take place in a secure, controlled environment with appropriate security measures in place to protect the central server; and o The algorithms behind the generation of the codes should be protected from unauthorised parties and updated regularly. 	
	<p>Evidence that the communications between the actors have been intercepted by an unauthorised party.</p>	<p>All the communication channels must be securely encrypted. Authentication of the stakeholders must use state-of-the-art security features.</p>	<p>The data security area of each party; During the audits performed by the competent authorities.</p>
	<p>Unauthorised parties receive a set of serial numbers.</p>	<p>The ID Issuer shall send the serial numbers generated only to those authorised wholesalers and distributors that requested the codes.</p>	<p>The system shall be allowed to respond to data queries to obtain information from the registry management in order to trace all the requests for serial numbers received and answered.</p>
	<p>Misalignment between the serial numbers generated and the aggregation packaging levels marked.</p>	<p>The Data Storage receives for the first time the serial numbers generated for the re-aggregation packaging levels, which are associated to a specific wholesaler or distributor. This information will be later validated at the moment of scanning the data carriers.</p>	<p>Economic operator; Data Storage Solution Provider. During the audits performed by the competent authorities.</p>
<p>10.2. Generation of Data Carrier for the re-aggregation activities</p>	<p>Lack of robustness of the unique identifiers.</p>	<p>Each of the unique identifiers created is unique due to its configuration ('primary information' + 'serial number' + 'ID Issuer identifier' + 'secondary information'). Each of the unique identifiers is linked to a specific manufacturer or importer and to a production line and date, contributing to the traceability of each of the unit packets marked.</p> <p>The serial number shall be a numeric or alphanumeric sequence of a maximum 20 characters, generated by a</p>	<p>The configuration of the unique identifiers (serial numbers + primary information + ID Issuer identifier + secondary information) will feed the data exploitation of the products tracing.</p>

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
		randomisation algorithm.	
10.3. Print / Affix the Data Carrier onto re-aggregation packaging levels	Misalignment between the serial numbers generated and the unit packets marked, or risk that not all the unit packets produced (or imported) are marked with a unique identifier.	Wholesalers and distributors that wish to re-aggregate are obliged to install equipment to count output, as well as devices to control, register, record and transmit the quantities of re-aggregation packaging levels marked.	During the audits, the compliance of the equipment installed in the production lines will be monitored, assessed, audited and approved.
	Outages of the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to print/affix the data carriers.	Tobacco wholesalers and distributors who wish to perform re-aggregation activities are obliged to install equipment to count output, as well as devices to control, register, record and transmit the quantities of packs produced.	During the audits, the compliance of the equipment installed in the production lines will be monitored, assessed, audited and approved.
10.4. Scan and report the Data Carriers	Communication failure: problems in the messaging from the wholesalers and distributors to the Data Storage. Connection to the Data Storage fails and the scanners are not able to connect to the Data Storage.	The scanners must transmit to the Data Storage the information contained in all the data carriers scanned in the production lines. Only those serial numbers scanned and transmitted to the Data Storage will be activated and considered as valid to be used through the supply chain. Communication redundancy solution shall be applied in order to allow an alternative way to conclude the data exchange.	The infrastructure support area of each party.
	Evidence that the communications between the actors have been intercepted by an unauthorised party.	All the communication channels must be securely encrypted. Authentication of the stakeholders must use state-of-the-art security features.	The data security area of each party; During the audits performed by the competent authorities.

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
	Validation of the serial numbers generated, the aggregation packaging levels marked and the total production (or imports).	<p>At this point, the Data Storage proceeds to the verification of the serial numbers generated, used and not used. The serial numbers generated are considered valid if they have been duly scanned by the correct wholesaler or distributor within the expiry date of each of the serial numbers.</p> <p>An alert is sent to the competent authorities, informing if there are discrepancies between serial numbers generated and data carriers scanned:</p> <ul style="list-style-type: none"> - Data carriers scanned with wrong serial numbers (not generated by the ID Issuer or generated for another date, wholesaler, distributor or production line). - Serial numbers generated and not used, which must be therefore considered as not valid for use during the supply chain. 	Economic operators; Data Storage Solution Provider; During the audits performed by the competent authorities.
11.1. Dispatch (exit) of tobacco products and transmission	Outages of the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to scan the data carriers.	Products will not be allowed to leave the responsibility of the wholesaler/distributor until an acknowledgement has been received from the Data Storage, confirming that the reporting message has been received and understood.	
	<p>Communication failure: problems in the messaging from the wholesalers and distributors to the Data Storage.</p> <p>Connection to the Data Storage fails and the scanners are not able to connect to the Data Storage.</p>	<p>Before the exit of the tobacco products from their possession, wholesalers and distributors shall report this movement to the Data Storage.</p> <p>A communication redundancy solution shall be applied in order to allow an alternative way to conclude the data exchange.</p>	The infrastructure support area of each party.
	Evidence that the communications between the actors have been intercepted by an unauthorised party.	All the communication channels must be securely encrypted. Authentication of the stakeholders must use state-of-the-art security features.	The data security area of each party; During the audits performed by the competent authorities.
	Validation that the traceability information reported is correct (IN-	The Data Storage keeps records of the exit of the tobacco product from the possession of	Economic operators; Data Storage Solution Provider; During the audits performed by

	Integrity problem (Disruption)	Control Mechanisms	
		Control components of the system	Supervision
	OUT principle).	the wholesalers and distributors, together with all other relevant dispatch information. The Data Storage proceeds to the validation of the dispatch information. In case of discrepancies between the dispatch information and other data stored previously, the Data Storage notifies the competent authorities.	the competent authorities.

1.7. Contingency plans

1.7.1. Introduction

Information systems are vital to the functioning of the Tracking and Tracing System, its mission and its business processes. Therefore, it is critical that services provided by the system are able to operate effectively without excessive interruption.

This Information System Contingency Plan (ISCP) establishes comprehensive procedures to recover the Tracking and Tracing System quickly and effectively after a service disruption.

1.7.1.1. Background

This ISCP establishes procedures to recover the Tracking and Tracing System after a disruption. The following recovery plan objectives have been established:

- Maximise the effectiveness of contingency operations through an established plan that consists of the following phases:
 - Activation and notification phase to activate the plan and determine the extent of damage;
 - Recovery phase to restore the Tracking and Tracing System operations; and
 - Reconstitution phase to ensure that the Tracking and Tracing System is validated through testing and that normal operations are resumed.
- Identify the activities, resources, and procedures to carry out the Tracking and Tracing System processing requirements during prolonged interruptions of normal operations.
- Assign responsibilities to designated stakeholders and provide guidance for recovering the Tracking and Tracing System during prolonged interruptions of normal operations.
- Ensure coordination with all stakeholders responsible for contingency planning measures.

1.7.2. Concept of operations

This section provides details about the Tracking and Tracing System, an overview of the three phases of the ISCP (activation and notification, recovery, and reconstitution), and a description of the roles and responsibilities during a contingency activation.

1.7.2.1. System description

The Tracking and Tracing System is composed of combined Data Storage (centralised for surveillance and decentralised for recording per manufacturer/importer), where all the data related to the tracking and tracing of the tobacco products manufactured in the European Union (and those manufactured outside of the EU, but destined for or placed on the EU market) will be stored.

To enable this recording, each unit of tobacco product shall be marked with a unique identifier. One of the elements of the unique identifier – the serial number – shall be generated by an ID Issuer, independent from the industry and under the control and mandate of the competent authorities.

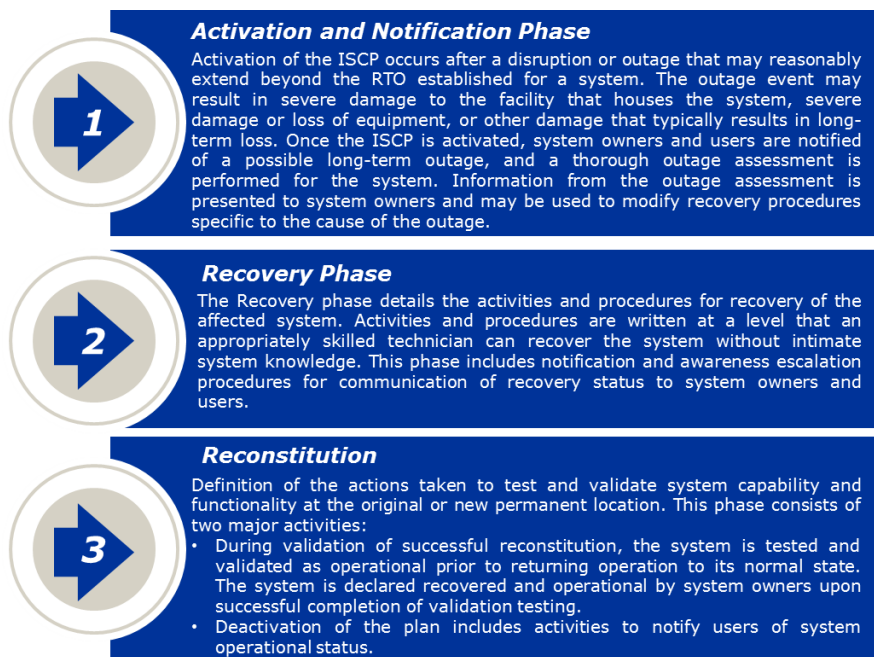
The unique identifiers (containing the serial number and product information) shall be printed or affixed to the tobacco products by the industry in the form of a data carrier. All movements of tobacco products through the supply chain (from the manufacturer to the last economic operator before the first retail outlet) shall be recorded in the Data Storage. 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, shall be recorded by the economic operators through the scanning of the data carriers.

Distributors and wholesalers shall also be able to mark the re-aggregation packaging levels that they may create in the context of their activities.

1.7.2.2. Overview of three phases

This ISCP has been developed to recover and reconstitute the Tracking and Tracing System using a three-phased approach. This approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximise the effectiveness and minimise system outage time due to errors and omissions.

The three system recovery phases are:



1.7.3. Activation and notification

The activation and notification phase defines initial actions to be taken once a disruption in the Tracking and Tracing System has been detected or appears to be imminent. This phase includes activities to notify the corresponding stakeholders, conduct an outage assessment, and activate the ISCP.

The Tracking and Tracing System ISCP may be activated if one or more of the disruptions are detected or appear to be imminent.

1.7.3.1. Notification

The first step upon activation of the ISCP is notification of appropriate mission/business and system support personnel. Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, and expected recovery time.

For the Tracking and Tracing System, the persons or roles in charge of activating the ISCP (according to the table above) must notify of the disruption as soon as it is detected or appears to be imminent. The notification must be sent to all other users that may be affected by that disruption. The notifications must contain the following information:

- Actor who makes the initial notification
- Actor(s) to whom the notification is addressed
- The outage/disruption and its location
- Cause of the outage/disruption (if known)
- Identification of potential for additional disruption or damage
- If applicable, notation of items that will need to be replaced and estimated time to restore service to normal operations

The selected method of notification shall allow keeping records of these notifications (e.g. email blasts in a secured environment). When needed and additionally, call trees² can be established (depending on the urgency of the notifications or whether multiple actors need to be notified).

1.7.4. Recovery

The recovery phase provides formal recovery operations that begin after the ISCP has been activated, outage assessments have been completed (if possible), stakeholders have been notified, and appropriate teams have been mobilised. The recovery phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. Upon completion of the recovery phase, the Tracking and Tracing System will be functional and capable of performing the functions identified in this plan (System Description).

1.7.4.1. Sequence of recovery activities

The following activities will occur during the recovery of the Tracking and Tracing System (with the persons or roles that activate the ISCP):

	Integrity problem (disruption)	Activation by	Recovery activities
0.1. Integration of the Security Features	Evidence that the security features have been copied by unauthorised parties (i.e. smugglers).	Competent authorities Manufacturers / importers Wholesalers / distributors	Application of Rotation Rules (for more detail please check Chapter 'Rotation Rules').
	Security feature not able to be authenticated by one method.	Competent authorities Manufacturers / importers Wholesalers / distributors	There are multiple ways for the competent authorities to authenticate a security feature, and whichever security elements are implemented, they must be given access to them: -Naked eye or mobile phone. -Yes/ No devices: Devices that provide immediate answer (Yes or No) on the presence or not of specific markers (covert feature) incorporated as part of the security feature. -Dedicated electronic devices: More reliable than mobile phones, these devices feature specific functionalities allowing further information for enhanced verification. -Filter, UV lamp, magnifier: Used by the competent authorities to verify semi-covert security features. -Laboratory equipment: Use of knowledge and dedicated scientific methods to validate the authentication elements or intrinsic properties of the material good.
	Production of security features not secure.	Competent authorities Manufacturers / importers Wholesalers / distributors	Full reconciliation at each stage of the production process with records maintained to account for all security material usage. The audit trail should be to a sufficient level of detail to account for every unit of security material used in the production and should be independently audited by persons who are not directly involved in the production. Records should be certified at a level of supervision to ensure accountability is kept of the destruction of all

² A call tree, sometimes referred to as a phone tree, call list, phone chain or text chain, is a telecommunications chain for notifying specific individuals of an event. Call trees, which are an important component of every disaster recovery plan, are especially helpful if an organisation needs to reach key personnel after hours to notify them of a problem.

	Integrity problem (disruption)	Activation by	Recovery activities
			security waste material and spoiled security feature items.
	Security features not secure during the transport	Competent authorities of the Member Manufacturers / importers Wholesalers / distributors	There are currently secure supply chain logistics for both inputs to the security feature, and control of storage and distribution itself. These can be maintained to guarantee the secure transport of the security features and/or the necessary supplies to the manufacturers' facilities.
	Security features storage not secure	Competent authorities Manufacturers / importers Wholesalers / distributors	Tax stamp ordering and logistics processes that provide control of labels/ stamps of value are currently established and in operation in most Member States today and can serve as a model for security features. Manufacturers operating in the EU would already be familiar with these processes, and can manage the reception, storage and waste management of the affixed security features elements. It is anticipated that as the distribution model has already been proven, that the logistics infrastructure could be setup in those Member States that do not currently have tax stamp programmes.
1.1. Generate the Serial numbers	Connection to the ID Issuer fails and the manufacturers and importers are not able to request serial numbers Communication failure: problems in the exchange from the manufacturers and importers to the ID Issuer and/or from the ID Issuer to the manufacturers and importers	Manufacturers / importers ID Issuer	As a part of the process of selecting an ID Issuer entity, each tenderer shall provide their contingency plan to ensure the continuity of the service. The robustness of these contingency plans shall be assessed by the competent authorities, together with their independence and technical capabilities. If the problem is on the ID Issuer side, the contingency plan of the ID Issuer shall be activated. Otherwise the economic operator shall proceed to re-establish the communication.
	Outages on the equipment and tools of the Tracking and Tracing System: the ID Issuer is temporarily unable to generate the serial numbers Risk of generating duplicates of the serial numbers (ID Issuer provides a serial number and the surveillance system reports that the generated UID already exists)	Competent authorities ID Issuer	As a part of the process of selecting an ID Issuer entity, each tenderer shall provide their contingency plan to ensure the continuity of the service. The robustness of these contingency plans shall be assessed by the competent authorities, together with their independence and technical capabilities. In this case, the contingency plan of the ID Issuer shall be activated.
	Evidence that the communications between the actors have been intercepted by an unauthorised party	All actors	As a part of the process of selecting the ID Issuer entity, each tenderer shall provide their data security capabilities to ensure the secure data exchange. The robustness of these capabilities shall be assessed by the competent authorities, together with their independence and technical capabilities. The ID Issuer shall review the data security policy and implement applicable solutions to prevent such problems.

	Integrity problem (disruption)	Activation by	Recovery activities
	Unauthorised parties receive the set of serial numbers	All actors	As soon as this integrity breach has been identified, the UIDs generated and received by the unauthorised parties shall be identified and the process of deactivation of the UIDs shall be triggered.
	Misalignment between the serial numbers generated and the unit packets marked	Surveillance Data Storage provider Competent authorities	As soon as this integrity breach has been identified, the UIDs generated and received by the unauthorised parties shall be identified and the process of deactivation of the UIDs shall be triggered. The competent authorities must be notified.
2.1. Print/Affix the data carriers onto Unit Packets	Misalignment between the serial numbers generated and the unit packets marked, or risk that not all the unit packets produced (or imported) are marked with a unique identifier	Manufacturers / importers	It is the responsibility of the manufacturers and importers to put in place mechanisms to restore the functionalities of the printers: o Fixing the current equipment in use; or o Replacing the malfunctioning printers. In case of replacement, a notification shall be sent to the competent authorities, notifying of: printer replaced, new printer installed, reason of the replacement and production line. Competent authorities may wish to visit the production line to ensure compliance with the requirements set.
	Outages on the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to print/affix the data carriers.	Manufacturers / importers	
3.1. Scan the data carriers	Risk that not all the unit packets produced (or imported) are scanned and reported	Independent third parties in charge of the anti-tampering devices of the scanners Manufacturers/ Importers	It is the responsibility of the manufacturers and importers to put in place mechanisms to restore the functionalities of the scanners: o Fixing the current equipment in use; or o Replacing the malfunctioning scanners. When this ISCP is activated, the independent third parties in charge of the anti-tampering devices installed must be notified and their assistance required. The independent third party must be present and approve any manipulation, fix or replacement of the scanners used to activate the unit packet marked. The competent authorities must be informed of any manipulation or replacement of the scanners installed in the production lines.
	Outages on the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to scan the data carriers.	Independent third parties in charge of the anti-tampering devices of the scanners Manufacturers/ Importers	

	Integrity problem (disruption)	Activation by	Recovery activities
3.2. Report the UIDs	<p>Communication failure: problems in the messaging from the manufacturers and importers to the Data Storage.</p> <p>Connection to the data storage fails and the scanners are not able to connect to the data Storage.</p>	<p>Manufacturers/ Importers</p> <p>Data Storage Provider</p>	<p>As a part of the process of selecting the Data Storage Provider entity, each tenderer shall provide their contingency plan to ensure the continuity of the service. The robustness of these contingency plans shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>If the problem is at the Data Storage provider side, the contingency plan of the Data Storage provider shall be activated. Otherwise the economic operator shall proceed to re-establish the communication.</p>
	<p>Evidence that the communications between the actors have been intercepted by an unauthorised party.</p>	<p>All actors</p>	<p>As a part of the process of selecting the Data Storage provider, each tenderer shall provide their data security capabilities to ensure the secure data exchange. The robustness of these capabilities shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>The Data Storage provider shall review the data security policy and implement applicable solutions to prevent such problems.</p>
	<p>Validation of the serial numbers generated, the unit packets marked and the total production (or imports)</p>	<p>Surveillance Data Storage provider</p> <p>Competent authorities</p>	<p>As soon as this integrity breach has been identified, the discrepancies shall be identified and the competent authorities must be notified.</p>
4.1. Generate the serial numbers	<p>Outages on the equipment and tools of the Tracking and Tracing System: the ID Issuer is temporarily unable to generate the serial numbers.</p> <p>Risk of generating duplicates of the serial numbers (ID Issuer provides a serial number and the Surveillance Data Storage reports that the generated UID already exists).</p>	<p>Competent authorities</p> <p>ID Issuer</p>	<p>As a part of the process of selecting the ID Issuer entity, each tenderer shall provide their contingency plan to ensure the continuity of the service. The robustness of these contingency plans shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>In this case, the contingency plan of the ID Issuer shall be activated.</p>
	<p>Evidence that the communications between the actors have been intercepted by an unauthorised party.</p>	<p>All actors</p>	<p>As a part of the process of selecting the ID Issuer entity, each tenderer shall provide their data security capabilities to ensure the secure data exchange. The robustness of these capabilities shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>The ID Issuer shall review the data security policy and implement applicable solutions to prevent such problems.</p>

	Integrity problem (disruption)	Activation by	Recovery activities
	Unauthorised parties receive the set of serial numbers.	All actors	As soon as this integrity breach has been identified, the UIDs generated and received by the unauthorised parties shall be identified and the process of deactivation of the UIDs shall be triggered.
	Misalignment between the serial numbers generated and the unit packets marked.	Surveillance Data Storage provider Competent authorities	As soon as this integrity breach has been identified, the UIDs generated and received by the unauthorised parties shall be identified and the process of deactivation of the UIDs shall be triggered. The competent authorities must be notified.
5.1. Print / Affix the data carrier onto aggregation packaging levels	Misalignment between the serial numbers generated and the unit packets marked, or risk that not all the unit packets produced (or imported) are marked with a unique identifier	Manufacturers / importers	It is the responsibility of the manufacturers and importers to put in place mechanisms to restore the functionalities of the printers: o Fixing the current equipment in use; or o Replacing the malfunctioning printers. In case of replacement, a notification shall be sent to the competent authorities, notifying of: printer replaced, new printer installed, reason of the replacement and production line. Competent authorities may wish to visit the production line to ensure compliance with the requirements set.
	Outages on the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to print/affix the data carriers.	Manufacturers / importers	
6.1. Scan the data carriers	Risk that not all the unit packets produced (or imported) are scanned and reported	Independent third parties in charge of the anti-tampering devices of the scanners Manufacturers/ Importers	It is the responsibility of the manufacturers and importers to put in place mechanisms to restore the functionalities of the scanners: o Fixing the current equipment in use; or o Replacing the malfunctioning scanners. When this ISCP is activated, the independent third parties in charge of the anti-tampering devices installed must be notified and their assistance required. The independent third party must be present and approve any manipulation, fix or replacement of the scanners used to activate the unit packet marked. The competent authorities must be informed of any manipulation or replacement of the scanners installed in the production lines.
	Outages on the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to scan the data carriers.	Independent third parties in charge of the anti-tampering devices of the scanners Manufacturers/ Importers	

	Integrity problem (disruption)	Activation by	Recovery activities
6.2. Report the UIDs	<p>Communication failure: problems in the messaging from the manufacturers and importers to the Data Storage.</p> <p>Connection to the Data Storage fails and the scanners are not able to connect to the Data Storage.</p>	<p>Manufacturers/ Importers</p> <p>Data Storage(s) Provider(s)</p>	<p>As a part of the process of selecting the Data Storage provider entity, each tenderer shall provide their contingency plan to ensure the continuity of the service. The robustness of these contingency plans shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>If the problem is on the Data Storage provider side, the contingency plan of the Data Storage provider shall be activated. Otherwise the economic operator shall proceed to re-establish the communication.</p>
	<p>Evidence that the communications between the actors have been intercepted by an unauthorised party.</p>	<p>All actors</p>	<p>As a part of the process of selecting the Data Storage Provider, each tenderer shall provide their data security capabilities to ensure the secure data exchange. The robustness of these capabilities shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>The Data Storage provider shall review the data security policy and implement applicable solutions to stop such problems.</p>
	<p>Validation of the serial numbers generated, the aggregation packaging levels marked and the total production (or imports)</p>	<p>Surveillance Data Storage provider</p> <p>Competent authorities</p>	<p>As soon as this integrity breach has been identified, the discrepancies shall be identified and the competent authorities must be notified.</p>
7.1. Dispatch (exit) of the tobacco products and transmission	<p>Outages on the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to scan the data carriers.</p>	<p>Independent third parties in charge of the anti-tampering devices of the scanners</p> <p>Manufacturers / importers</p>	<p>As a good practice, it is advised that all manufacturers and importers have a sufficient back-up set of scanners to make use of in case of breakdown or outage of the scanners used.</p> <p>In any case, it is the responsibility of the manufacturers and importers to put in place mechanisms to restore the functionalities of the scanners.</p>
	<p>Communication failure: problems in the messaging from the manufacturers and importers to the Data Storage.</p> <p>Connection to the Data Storage fails and the scanners are not able to connect to the Data Storage.</p>	<p>Manufacturers/ Importers</p> <p>Data Storage Provider</p>	<p>As a part of the process of selecting the Data Storage provider entity, each tenderer shall provide their contingency plan to ensure the continuity of the service. The robustness of these contingency plans shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>If the problem is at the Data Storage provider side, the contingency plan of the Data Storage provider shall be activated. Otherwise the economic operator shall proceed to re-establish the communication.</p>
	<p>Evidence that the communications between the actors have been intercepted by an unauthorised party.</p>	<p>All actors</p>	<p>As a part of the process of selecting the Data Storage provider, each tenderer shall provide their data security capabilities to ensure the secure data exchange. The robustness of these capabilities shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>The Data Storage provider shall review the data security policy and implement applicable solutions to prevent such problems.</p>

	Integrity problem (disruption)	Activation by	Recovery activities
	Validation that the traceability information reported is correct (IN-OUT principle)	Economic Operator Data Storage Provider Competent authorities	As soon as this integrity breach has been identified, the discrepancies shall be identified and the competent authorities must be notified.
8.1. Reception (entry) of the tobacco products and transmission	Outages on the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to scan the data carriers.	Wholesalers / distributors	<p>According to the TPD, manufacturers and importers shall provide all economic operators involved in the trade of tobacco products with the equipment necessary for the recording of the tobacco products. It should be considered whether one back-up set of scanners may in this context also be required</p> <p>In case the ISCP is activated due to unavailability of the scanners, manufacturers and importers shall replace the scanners within the shortest delay possible.</p> <p>In the meantime, the wholesalers and distributors shall make use of the back-up scanning equipment at their disposal.</p>
	<p>Communication failure: problems in the messaging from the wholesalers and distributors to the Data Storage.</p> <p>Connection to the Data Storage fails and the scanners are not able to connect to the Data Storage.</p>	<p>Wholesalers / distributors</p> <p>Surveillance Data Storage Provider</p>	<p>As a part of the process of selecting the Data Storage provider entity, each tenderer shall provide their contingency plan to ensure the continuity of the service. The robustness of these contingency plans shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>If the problem is on the Data Storage provider side, the contingency plan of the Data Storage provider shall be activated. Otherwise the economic operator shall proceed to re-establish the communication.</p>
	Evidence that the communications between the actors have been intercepted by an unauthorised party.	All actors	<p>As a part of the process of selecting the Data Storage provider, each tenderer shall provide their data security capabilities to ensure the secure data exchange. The robustness of these capabilities shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>The Data Storage provider shall review the data security policy and implement applicable solutions to prevent such problems.</p>
	Validation that the traceability information reported is correct (IN-OUT principle).	Surveillance Data Storage provider Competent authorities	As soon as this integrity breach has been identified, the discrepancies shall be identified and the competent authorities must be notified.

	Integrity problem (disruption)	Activation by	Recovery activities
10.1. Generation of the serial numbers for the re-aggregation activities	<p>Outages on the equipment and tools of the Tracking and Tracing System: the ID Issuer is temporarily unable to generate the serial numbers.</p> <p>Risk of generating duplicates of the serial numbers (ID Issuer provides a serial number and the surveillance system reports that the generated UID already exists).</p>	<p>Competent authorities</p> <p>ID Issuer</p>	<p>As a part of the process of selecting the ID Issuer entity, each tenderer shall provide their contingency plan to ensure the continuity of the service. The robustness of these contingency plans shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>In this case, the contingency plan of the ID Issuer shall be activated.</p>
	<p>Evidence that the communications between the actors have been intercepted by an unauthorised party.</p>	<p>All actors</p>	<p>As a part of the process of selecting the Data Storage provider, each tenderer shall provide their data security capabilities to ensure the secure data exchange. The robustness of these capabilities shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>The Data Storage provider shall review the data security policy and implement applicable solutions to prevent such problems.</p>
	<p>Unauthorised parties receive the set of serial numbers.</p>	<p>All actors</p>	<p>As soon as this integrity breach has been identified, the UIDs generated and received by the unauthorised parties shall be identified and the process of deactivation of the UIDs shall be triggered.</p> <p>The competent authorities must be notified.</p>
	<p>Misalignment between the serial numbers generated and the unit packets marked.</p>	<p>Surveillance Data Storage provider</p> <p>Competent authorities</p>	<p>As soon as this integrity breach has been identified, the UIDs generated and received by the unauthorised parties shall be identified and the process of deactivation of the UIDs shall be triggered.</p> <p>The competent authorities must be notified.</p>
10.3. Print / Affix the data carrier onto re-aggregation packaging levels	<p>Misalignment between the serial numbers generated and the unit packets marked, or risk that not all the unit packets produced (or imported) are marked with a unique identifier.</p>	<p>Wholesalers / distributors</p>	<p>It is the responsibility of the wholesalers and distributors wishing to re-aggregate to put in place mechanisms to restore the functionalities of the printers:</p> <ul style="list-style-type: none"> o Fixing the current equipment in use; or o Replacing the malfunctioning printers. <p>In case of replacement, a notification shall be sent to the competent authorities, notifying: printer replaced, new printer installed, reason of the replacement and production line. Competent authorities may wish to visit the production line to ensure compliance with the requirements set.</p>
	<p>Outages on the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to print/affix the data carriers.</p>	<p>Wholesalers/ Distributors</p>	<p>It is the responsibility of the wholesalers and distributors to put in place mechanisms to restore the functionalities of the printers:</p> <ul style="list-style-type: none"> o Fixing the current equipment in use; or o Replacing the malfunctioning printers. <p>In case of replacement, a notification shall be sent to the competent authorities, notifying: printer replaced, new printer installed, reason of the replacement and production line. Competent authorities may wish to visit the production line to ensure compliance with the requirements set.</p>

	Integrity problem (disruption)	Activation by	Recovery activities
10.4. Scan and report the data carriers	Outages on the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to scan the data carriers.	Wholesalers / distributors	<p>According to the TPD, manufacturers and importers shall provide all economic operators involved in the trade of tobacco products with the equipment that is necessary for the recording of the tobacco products. It should be considered whether one back-up set of scanners may in this context also be required.</p> <p>In case the ISCP is activated due to unavailability of the scanners, manufacturers and importers shall replace the scanners within the shortest delay possible.</p> <p>In the meantime, the wholesalers and distributors shall make use of the back-up scanning equipment at their disposal.</p>
	<p>Communication failure: problems in the messaging from the wholesalers and distributors to the Data Storage.</p> <p>Connection to the Data Storage fails and the scanners are not able to connect to the Data Storage.</p>	<p>Wholesalers / distributors</p> <p>Surveillance Data Storage Provider</p>	<p>As a part of the process of selecting the Data Storage provider entity, each tenderer shall provide their contingency plan to ensure the continuity of the service. The robustness of these contingency plans shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>If the problem is at the Data Storage provider side, the contingency plan of the Data Storage provider shall be activated. Otherwise the economic operator shall proceed to re-establish the communication.</p>
	Evidence that the communications between the actors have been intercepted by an unauthorised party.	All actors	<p>As a part of the process of selecting the Data Storage provider, each tenderer shall provide their data security capabilities to ensure the secure data exchange. The robustness of these capabilities shall be assessed by the competent authorities, together with their independence and technical capabilities.</p> <p>The Data Storage provider shall review the data security policy and implement applicable solutions to prevent such problems.</p>
	Validation of the serial numbers generated, the aggregation packaging levels marked and the total production (or imports).	<p>Surveillance Data Storage provider</p> <p>Competent authorities</p>	As soon as this integrity breach has been identified, the discrepancies shall be identified and the competent authorities must be notified.
11.1. Dispatch (exit) of tobacco products and transmission	Outages on the equipment and tools of the Tracking and Tracing System: temporary unavailability or interruption of the operation of the equipment used to scan the data carriers.	Wholesalers/ distributors	<p>According to the TPD, manufacturers and importers shall provide all economic operators involved in the trade of tobacco products with the equipment that is necessary for the recording of the tobacco products. It should be considered whether one back-up set of scanners may in this context also be required.</p> <p>In case the ISCP is activated due to unavailability of the scanners, manufacturers and importers shall replace the scanners within the shortest delay possible.</p> <p>In the meantime, the wholesalers and distributors shall make use of the back-up scanning equipment at their disposal.</p>

	Integrity problem (disruption)	Activation by	Recovery activities
	Communication failure: problems in the messaging from the wholesalers and distributors to the Data Storage.	Wholesalers / distributors	As a part of the process of selecting the Data Storage provider entity, each tenderer shall provide their contingency plan to ensure the continuity of the service. The robustness of these contingency plans shall be assessed by the competent authorities, together with their independence and technical capabilities.
	Connection to the Data Storage fails and the scanners are not able to connect to the Data Storage.	Surveillance Data Storage Provider	If the problem is at the Data Storage provider side, the contingency plan of the Data Storage provider shall be activated. Otherwise the economic operator shall proceed to re-establish the communication.
	Evidence that the communications between the actors have been intercepted by an unauthorised party.	All actors	As a part of the process of selecting the Data Storage provider, each tenderer shall provide their data security capabilities to ensure the secure data exchange. The robustness of these capabilities shall be assessed by the competent authorities, together with their independence and technical capabilities. The Data Storage provider shall review the data security policy and implement applicable solutions to prevent such problems.
	Validation that the traceability information reported is correct (IN-OUT principle)	Surveillance Data Storage Provider	As soon as this integrity breach has been identified, the discrepancies shall be identified and the competent authorities must be notified.

1.7.4.2. Recovery escalation notices/awareness

When needed, notifications for escalation notices shall be sent to the competent authorities and to other actors involved in the recovery efforts.

These notifications shall include Member State awareness and recurrent re-assessment of the situation (if the assessment differs from the assessment made during the activation and notification phase).

1.7.5. Reconstitution

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the system has undergone significant changes and will require reassessment and reauthorisation. This phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

1.7.5.1. Validation data testing

Validation data testing is the process of testing and validating data to ensure that data files or databases have been recovered completely at the permanent location. The tests shall check that correct procedures are used and shall determine that the data is complete and current up to the last available backup. Several tests shall be completed to

assure the total recovery of the data, such as the verification that the last known complete transaction was updated in the database, or comparing a database audit log to the recovered database to make sure all transactions were properly updated.

1.7.5.2. Validation functionality testing

Validation functionality testing is the process of verifying that the functionalities of the Tracking and Tracing System have been tested, and the system is ready to return to normal operations. To validate the functionalities of the system, the actor that has activated the ISCP must perform validation procedures to ensure that the system is operating correctly, once all the recovery activities have been completed.

An example of a functional test may be manufacturers and importers trying to print data carriers again after a printer has been fixed or replaced (disruptions with ID 02-01 and 06-01); or the ID Issuer generating serial numbers after the recovery activities of the contingency plan have been completed, after temporary unavailability of the ID Issuer to generate serial numbers (disruption with ID 01-03, 05-03 and 11-03).

1.7.5.3. Recovery declaration

Upon successful completion of testing and validation, the actor that made the initial notification (and thus activated the ISCP) will formally declare the recovery efforts to be complete, and that the Tracking and Tracing System has returned to normal operations. The competent authorities shall be notified of this declaration.

1.7.5.4. Notifications (users)

Upon return to normal system operations, Tracking and Tracing System users will be notified, using predetermined notification procedures.

1.7.5.5. Data backup

As soon as reasonably possible after recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups. Procedures shall be followed to ensure that a full system backup is conducted within a reasonable timeframe, ideally before the next scheduled backup period.

1.7.5.6. Event documentation

It is important that all recovery events are well documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learnt for inclusion and update to the ISCP. It is the responsibility of each ISCP team or individual to document their actions during the recovery and reconstitution effort. For each of the disruptions and after a contingency activation, the actors should generate and collect the following types of documentation:

- *Activity logs (including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities);*
- *Functionality and data testing results;*
- *Lessons learnt documentation; and*
- *After Action Report.*

1.7.5.7. Deactivation

Once all activities have been completed and documentation has been updated, a formal deactivation notice shall be issued and deactivate the ISCP recovery and reconstitution effort. Notification of this declaration will be provided to all actors involved and affected by the disruption/outage.

1.8. System security plan

1.8.1. Introduction

The objective of this section is to propose a methodology and a candidate group of requirements to be taken into account in the Tracking and Tracing System, thus achieving a secure platform that will allow a safe and appropriate access to information and functionalities.

As a result of the security analysis process, the security plan should contain a high level risk analysis to clarify the **risk of the assets** of the system and the necessary **countermeasures**.

1.8.2. Scope

The scope and the security recommendations proposed are aligned with the technological recommendations defined in the standard decision 3602 (European Commission - Decision 3602, 2006) and the OWASP (OWASP - Secure Coding, 2016).

The Tracking and Tracing System is composed of the following main groups of data elements:

- A. Unique identifier of unit packet of tobacco products:
 - date and place of manufacturing
 - manufacturing facility
 - machine used to manufacture the tobacco products
 - production shift or time of manufacture
 - product description
 - serial number in the Tracking and Tracing System
 - importer into the Union, where applicable
 - Tracking:
 - intended market of retail sale

- intended shipment route
- actual shipment route from manufacturing to the first retail outlet, including all warehouses used as well as the shipment date, shipment destination, point of departure, and consignee
- Trade:
 - identity of all purchasers from manufacturing to the first retail outlet
 - invoice, order number and payment records of all purchasers from manufacturing to the first retail outlet

B. Event data

- serial number generation
- unit packet production
- aggregation packaging
- dispatch
- receipt

At this stage, this data information is considered the main asset along with the individual solutions (i.e. Primary Data Storage, Surveillance Data Storage and ID Issuer solution) that comprise the System. No physical equipment, communications support or locations are considered as assets.

The providers who establish the individual solutions of the System shall provide details of their system security plan and include additional security factors applied to the specificities, responsibilities, and any necessary development related to each individual solution (i.e. Primary Data Storage, Surveillance Data Storage and ID Issuer solutions).

In the sections below, the following topics will be described as a blue print for the solution providers to develop a system security plan:

- Details regarding the **methodology** proposed to implement the system security plan.
- Candidate **security requirements**.

1.8.3. Security needs

The security needs of the information systems and the information processed therein are expressed in terms of their level of confidentiality, integrity and availability. The classification of the system (standard or specific) is determined on the basis of these needs. The definition of the levels of confidentiality, integrity and availability is included below.

IDENTIFICATION OF THE LEVEL OF CONFIDENTIALITY OF INFORMATION SYSTEMS	
PUBLIC	Information system or information whose public disclosure would not damage the interests of the Commission, the other Institutions, the Member States or other parties;
LIMITED	Information system or information reserved for a limited number of persons on a need-to-know basis and whose disclosure to unauthorised persons would be prejudicial to the Commission, other Institutions, Member States or other parties, but not to an extent serious enough to merit classification as laid down in paragraph 16.1 of the provisions on security. An additional marking may be attached for information at this level of security identifying the

		categories of persons or bodies who are the recipients of the information or authorised to access it. This category is further divided into 'basic' and 'high'.
LIMITED	BASIC	Information systems or information reserved for a limited number of persons on a need-to-know or need-to-access principle and whose disclosure to unauthorised persons would cause moderate prejudice to the Commission, other Institutions, Member States or other parties, but not to an extent serious enough to merit EU classification.
	HIGH	Information systems or information reserved for a limited number of persons on a need-to-know or need-to-access principle and whose disclosure to unauthorised persons would cause consequential prejudice to the Commission, other Institutions, Member States or other parties, but not to an extent serious enough to merit EU classification.

IDENTIFICATION OF THE LEVELS OF INTEGRITY OF INFORMATION SYSTEMS

MODERATE	Information or information systems whose loss of integrity might threaten the internal working of the Commission, other institutions, Member States or other parties; cases would include the non-application of the security rules without any outside impact or with limited outside impact, a threat to the achievement of the objectives of an action plan, or the appearance of significant organisational and operational problems within the Commission, other institutions, Member States or other parties without any outside impact.
CRITICAL	Information or information systems whose loss of availability might threaten the position of the Commission, other institutions, Member States or other parties; cases would include damage to the image of the Commission, other institutions, Member States or other parties or of other Institutions in the eyes of the Member States or the public, a very serious prejudice to legal or natural persons, a budget overrun or a substantial financial loss with very serious adverse consequences for the above authority's finances.
STRATEGIC	Information or information systems whose loss of integrity would be unacceptable to the Commission, other institutions, Member States or other parties because it might, for example, lead to the halting of the decision-making process, an adverse effect on important negotiations involving catastrophic political damage or financial losses, or the undermining of the Treaties or their application.

IDENTIFICATION OF THE LEVELS OF AVAILABILITY OF INFORMATION SYSTEMS

MODERATE	Information or information systems whose loss of availability might threaten the internal working of the Commission, other institutions, Member States or other parties; cases would include the non-application of the security rules without any outside impact or with limited outside impact, a threat to the achievement of the objectives of an action plan, or the appearance of significant organisational and operational problems within the Commission, other institutions, Member States or other parties without any outside impact.
CRITICAL	Information or information systems whose loss of availability might threaten the position of the Commission, other institutions, Member States or other parties; cases would include damage to the image of the Commission, other institutions, Member States or other parties in the eyes of the Member States or the public, a very serious prejudice to legal or natural persons, a budget overrun or a substantial financial loss with very serious adverse consequences for the above authority's finances.
STRATEGIC	Information or information systems whose loss of availability would be unacceptable to the Commission, other institutions, Member States or other parties because it might, for example, lead to the halting of the decision-making process, an adverse effect on important negotiations involving catastrophic political damage or financial losses, or the undermining of the Treaties or their application.

The output of the security evaluation is presented in the table below.

System	Confidentiality	Integrity	Availability
Tracking and Tracing System	Limited Basic	Critical	Critical

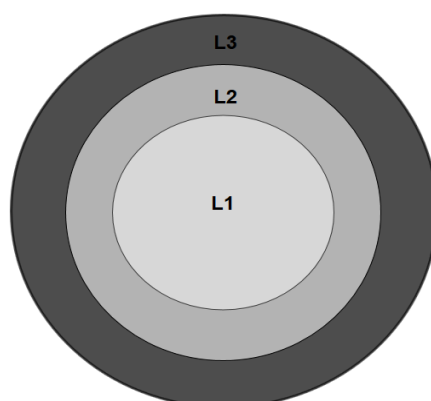
The justification of the confidentiality, integrity and availability levels is presented below:

- **Confidentiality:** The reason for this level is that data must only be accessible by competent authorities and auditors. Manufacturers, importers, wholesalers and distributors will have access to data only in duly justified cases when the Commission or the Member States may provide data.
- **Integrity:** Guaranteeing integrity is essential for the Tracking and Tracing System. The receipt of the communication must also be secured as a proof that the information was well received.
- **Availability:** In terms of information availability, the System and its information must be available. Any other case would be a failure according to Article 15 of the TPD.

The security needs of the Tracking and Tracing System are established following the methodology depicted in the figure below.

Confidentiality	Availability	Integrity	
<div style="border: 1px solid black; padding: 2px;">PUBLIC</div> <div style="border: 1px solid black; padding: 2px;">LIMITED BASIC</div>	<div style="border: 1px solid black; padding: 2px;">MODERATE</div>	<div style="border: 1px solid black; padding: 2px;">MODERATE</div>	L1
<div style="border: 1px solid black; padding: 2px;">LIMITED HIGH</div> <div style="border: 1px solid black; padding: 2px;">CONFIDENTIEL UE</div>	<div style="border: 1px solid black; padding: 2px;">CRITICAL</div>	<div style="border: 1px solid black; padding: 2px;">CRITICAL</div>	L2
<div style="border: 1px solid black; padding: 2px;">RESTREINT UE</div> <div style="border: 1px solid black; padding: 2px;">SECRET EU</div> <div style="border: 1px solid black; padding: 2px;">TOP SECRET EU</div>	<div style="border: 1px solid black; padding: 2px;">STRATEGIC</div>	<div style="border: 1px solid black; padding: 2px;">STRATEGIC</div>	L3

Regarding the levels, it is mandatory that the highest level cover the lower levels. For instance, if an application fits on level 3 (L3), the levels 1 and 2 controls must be applied in the same way as controls from level 3. The following chart depicts this concept:



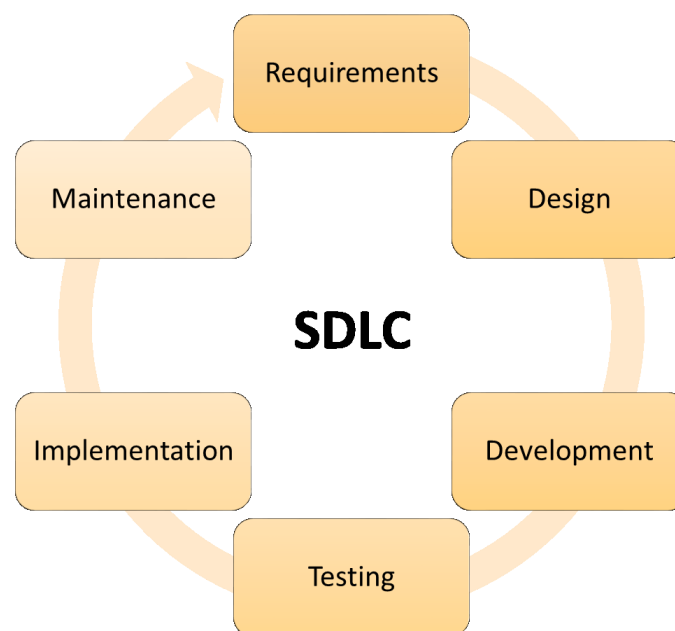
1.8.4. Proposed methodology

The proposed methodology to define the Tracking and Tracing System security plan is based on the systems development life cycle (SDLC), which is a conceptual model used in project management that describes the stages involved in an information system

development project, from an initial feasibility study through maintenance of the completed application.

This methodology provides a sequence of activities for system designers and developers to follow. It consists of a set of steps or phases in which each phase of the SDLC uses the results of the previous one.

The following image depicts the different phases of this methodology:



The phases of the SDLC, in which the output of each phase becomes the input for the next one, are described from a security point of view:

- **Requirements:** The initial development of an application must have the security design and comply with the security requirements established.
- **Design:** Risk analyses are performed to ensure that security and privacy issues are thoroughly mitigated by design. The use of attack surface reduction techniques and threat modelling improves the design coverage against known and potential threats.
- **Development:** The coding of an application must be secure, which is measured based on ensuring the security of the code and on preventing any vulnerabilities from breaking it.
- **Testing:** Brings all the pieces together into a special testing environment to check for errors and review that everything is working as expected in the previous phases.
- **Implementation:** The integration of the code with the infrastructure represents a delicate stage of the process where various vulnerabilities may appear. It is important to detect them as soon as possible.
- **Maintenance:** Simulation of case scenarios from the point of view of the attacker to detect vulnerabilities in the system, the application or any of the processes.

As part of the design phase, when additional design details of the System are developed, the following tasks must be performed according to the European Decision 3602 (European Commission - Decision 3602, 2006). In addition to this, in section 1.8.5 a set of candidate requirements to be considered by the solution provider has been proposed, including the following:

- Threat and vulnerability assessment
- The prioritised list of risk areas, justification and comments for the assigned priorities
- Definition of security countermeasures
- Risk Treatment Plan
- Residual Risk Statement
- Risk Assessment Report

1.8.5. Candidate security requirements

This section proposes a set of security requirements and controls to be planned and executed, related to the security aspects of the software lifecycles of the individual solutions of Tracking and Tracing System. These requirements are based on **OWASP** (Open Web Application Security Project - (OWASP - Secure Coding, 2016)). These requirements are related to security needs up to Level 2.

The candidate groups of topics to be considered as requirements when designing the System Security Plan are the following:

- Authentication
- Session management
- Authorisation
- Input validation
- Cryptography
- Secure communications
- Resources and file management
- Web services
- Error handling and logging management
- Data protection
- Software design requirements:
 - Application general architecture
 - Software design
 - Configuration
- Infrastructure requirements:
 - Network
 - Execution environment

- **Hardening**

2. DETAILED TECHNICAL SPECIFICATIONS FOR THE SUPPLY CHAIN ELEMENTS OF THE TRACKING AND TRACING SYSTEM

2.1. Unique identifier (at unit packet level)

2.1.1. Assessment of the requirements and composition of the unique identifier

This section introduces the proposed coding format for the information elements that shall form part of the unique identifier at unit packet level, as required by Article 15(2) of the TPD.

Since Article 15(2) of the TPD requires that nine different data elements form part of the unique identifier, certain challenges are posed:

- **Length of the unique identifier.** It is necessary to include a high number of data elements in the unique identifier. Furthermore, some of these elements have no direct mapping to datasets managed by international supply chain standards organisations. As such, the final size of the unique identifier risks being excessively large, which will have a negative impact on high-speed production lines. The optimal size of the unique identifier to be applied to the unit packet of tobacco products should not exceed 60 characters and preferably be closer to 40 characters.
- **Access to legible information** for competent authorities. However, the data elements that form part of the unique identifier can be previously encoded to reduce the length of the unique identifier. This suggests that use could be made of lookup tables as an instrument to decode and convert the codes into legible information for the competent authorities, thereby increasing the effectiveness of surveillance activities.

Hence, the Implementation Study has conducted an analysis, based on which it has proposed an optimal coding format for the unique identifier. This proposal meets the challenging information requirements of the TPD and minimises the impact on the speed of the printing equipment on the production lines.

The analysis uses the following methodological approach:

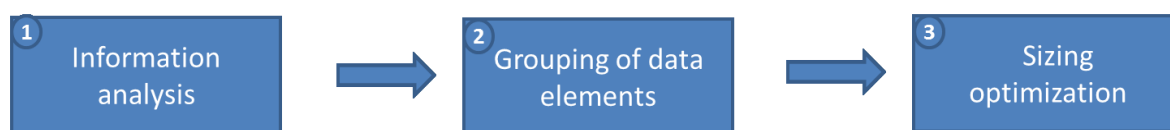


Figure 5: Methodological approach for the codification of the unique identifier

The goals for each stage are:

- Identifying different attributes that qualify and categorise the information.
- Grouping the information by clusters of elements in order to promote possible data relationships and synergies.
- Analysing different coding alternatives in order to optimise the sizing of the individual groups.

The unique identifier described in this section presents a specific syntax as a result of the analysis carried out, and deals with the two challenges previously posed – length of unique identifier and access to legible information. Nonetheless, this syntax may be modified by the ID Issuer as long as it does not affect the overall functionality of the Tracking and Tracing System.

2.1.1.1. Baseline

2.1.1.1.1. Directive 2014/40/EU requirements

Article 15(3) of the TPD sets out that the information contained in the table below shall form part of the unique identifier.

Element ID	TPD Request	TPD Article	Interpretation
ID01	Date of manufacturing	15(2a)	The day, month and year when the production took place.
ID02	Place of manufacturing	15(2a)	The country where the production took place.
ID03	Manufacturing facility	15(2b)	The identification of the manufacturing facility: owner and address.
ID04	Machine used to manufacture the tobacco products	15(2c)	The identification of the machine or group of machines inside the manufacturing facility.
ID05	Production shift or time of manufacture	15(2d)	Identification of the production shift or time when the production order is launched.
ID06	Product description	15(2e)	Unique identification of the product contained in the unit packet.
ID07	Intended market of retail sale	15(2f)	The identification of the country where the unit packet will be sold.
ID08	Intended shipment route	15(2g)	The list of countries that the unit packet can visit until it arrives to the first retail outlet.
ID09	Where applicable, the importer into the union	15(2h)	The identification of the importer of the unit packet if it comes from outside the EU. The identification of the importer should be unique (i.e. by CIF).

Table 1: Directive 2014/40/EU requirements

2.1.1.1.2. ID Issuer

The ID Issuer is the independent entity responsible for generating and issuing unique identifiers (see Main Report – Chapter 5: *Technical specifications for the Tracking and Tracing System*).

Among its duties, the ID Issuer keeps a registry for the identification codes of the elements of information requested by the TPD to form part of the unique identifier. It is also responsible of the generation and maintenance of the lookup tables, which enable the offline extraction of the information encoded in the unique identifiers.

2.1.1.1.3. Lookup tables

Lookup tables are the tools that enable users to encode a certain volume of information by using codes as identifiers, allowing a significant reduction of the number of digits needed to encode one or more registers of information (Radyakin, 2016).

Lookup tables are generally used to help with database normalisation for data that is relatively static, such as tables containing names of countries, cities, etc. The following image presents a lookup table schema:

Code	Machine	Location	...	Country
FTED3	Turbo 5043	Madrid	...	Spain
H89GE	Printer F45	Lyon	...	France
...
TY91S	Generic Series A	Rome	...	Italy

Table 2: Lookup table description

In order to ensure the correct functioning of the System, the ID Issuers are responsible of generating lookup tables and ensuring that they are kept up to date. It should be noted that this lookup registration process would be required for any facility/production line that manufactures tobacco products to be sold in the EU, even it is located outside the EU.

Along with the points mentioned above, security is a main challenge of the lookup tables, which are intended for use only by authorised personnel. By including some security features, such as prior identification before use, this objective can be accomplished.

Furthermore, once the needs and responsibilities of each lookup table's users are identified, it may not be necessary to download every table. Access to the specific information required may be sufficient.

In order to decode unique identifiers without accessing the database, the lookup tables should be downloaded into the devices used by MS enforcement authorities.

2.1.1.2. Information analysis

In order to facilitate the subsequent grouping of information, the elements of the unique identifier have been analysed according to the following criteria:

- Supply chain stage: Identifies which part of the supply chain the code is presenting information about.
- Factual information: Identifies the question category (When, Where, What, Who, Why) that may provide the requested information.
- Code variability: Identifies whether the information is known before the production process starts. The elements are categorised as 'static' when the information is fixed and known before the production, and 'dynamic' when it may vary.
- Veracity of information: Identifies whether the requested information is known before the printing process or not.

The following table shows the identification of these attributes for the batch of information requested.

Element ID	Information requested	Supply chain stage	Factual information	Code variability	Veracity of the information
ID02	Place of manufacturing	Manufacturing	Where	Static	Known
ID03	Manufacturing facility	Manufacturing	Where	Static	Known
ID04	Machine used to manufacture the tobacco products	Manufacturing	Where	Static	Known
ID06	Product description	Manufacturing	What	Static	Known
ID01	Date of manufacturing	Manufacturing	When	Dynamic	Known
ID05	Production shift or time of manufacture	Manufacturing	When	Dynamic	Known
ID07	Intended market of retail sale	Distribution	Where	Static	Intended
ID08	Intended shipment route	Distribution	Where	Static	Intended
ID09	Where applicable, the importer into the European Union	Distribution	Who	Static	Known

Table 3: Analysis of the elements of information

In addition to the information requested by the TPD, two new elements should be included in the unique identifier:

- ID Issuer identification code: since several ID Issuer solutions may be established, this element will enable their identification.
- Serial number: to ensure the uniqueness of the code.

2.1.1.3. Grouping of data elements

This stage aims at determining whether data elements have similarities, and therefore can be grouped into clusters under the same category. The overarching objective is to identify possible groups that include all the information requested by the TPD to form part of the unique identifier.

Based on the differences in the nature of the data elements, seven clusters have been identified:

- Location of the manufacturing activities
 - Place of manufacturing
 - Manufacturing facility
 - Machine used to manufacture the tobacco products
- Product identification
 - Product description

- Date and time of the manufacturing activities
 - Date of manufacture
 - Product shift or time of manufacture
- Shipment route information
 - Intended market of retail
 - Intended shipment route
- Importer into the European Union
- Serial number
- ID Issuer identification code

2.1.1.4. Sizing optimisation

The purpose of the sizing optimisation is twofold:

- **Minimise the length of the unique identifier** by optimising the individual length of each of the data elements that will form part of the unique identifier to be applied to the unit packet of tobacco products. This is important to avoid a negative impact on high-speed production lines.
- **Minimise the size of the lookup tables** by optimising the size of the fields that contain the readable information referred by the individual data elements of the unique identifier. This is important because the lookup tables will be downloaded by the competent authorities in their hand-held devices, which may have low memory resources.

2.1.1.4.1. Location of the manufacturing activities

The formation of the code that represents this group (location of the manufacturing activities) should take into account the following considerations:

- Global identification numbers such as GLN or GAIA (GS1, GS1 General Specifications, 2017) cannot be used (as a sub-part of the unique identifier code) because they introduce an excessive number of digits.
- The machines or groups of machines used to manufacture the tobacco products inside a manufacturing facility are arranged into production lines. The implementation team recommends that the production lines be uniquely identified.
- The production lines, by definition, are located inside a manufacturing facility, which in turn is located in a specific country. Therefore, the use of a code (alphanumeric digits) that identifies the production lines enables linking the rest of the information requested by the TPD (place of manufacturing and manufacturing facility). This grouping allows a reduction of the code length.
- To ensure that any equipment is able to read them (even in offline mode), the codes contained in the unique identifier lookup tables should be downloaded to the equipment.

Estimation of the code length

It is estimated that there are approximately 332 tobacco manufacturing facilities in the EU, containing 743 production lines (everis, 2017). Additionally, in order to estimate the number of production lines that may manufacture tobacco products for later consumption in the EU, and considering that consumption of tobacco products in the EU represents 8.4% of global consumption, the following assumptions are made:

- As consumption in the EU is 8.4% of the world total, this percentage also represents the number of EU production lines in the world total.
- A multiplicative factor of 10 is used to oversize the number of production lines and to provide enough capacity.
- Not all the production lines in the world will manufacture tobacco products for the EU.

The result of the estimation of the maximum number of production lines (outside the EU) that might provide tobacco products to the EU is 88,452. Thus, the capacity of the code must be higher than the total number of production lines (743 production lines inside the EU + 88,452 production lines outside the EU). However, this calculation is only an approximation of the maximum capacity, and only the production lines sending products to the EU need to be registered.

Additionally, the lookup table will contain the location of aggregation activities for the unique identifier at aggregation packaging level, resulting in a total of 95,500 records.

A four-digit alphanumeric code can contain 1.68 million records, a sufficient amount to encode all the production lines (5.6% over the total capacity).

In conclusion, an independent four-digit alphanumeric code can be used to contain all the information requested by the TPD regarding location of manufacturing activities in the unique identifier.

Element ID	Information requested	Code example	Number of characters
ID02	Place of manufacturing	A1B2	4
ID03	Manufacturing facility		
ID04	Machine used to manufacture the tobacco products		

Table 4: Example of location of manufacturing activities code

The next table shows an example of the lookup table layout, where the columns machine identifier, manufacturing facility, and country of origin include the information requested by the TPD. Additionally, an extra column is included: status (e.g. approved, pending approval, inactive or rejected).

Code	Machine identifier	Manufacturing facility	Country of origin	Status
RXA1	Ref 0023021	– Industries 1A2B, Inc. ABC street, number 4, Madrid, Spain, zip code 28045	Spain	Approved
YO53	Ref 0050177	– Industries 5Q84, Inc. RTY street, number 78, Lyon, France, zip code 69123	France	Pending approval

Table 5: Example of lookup table for location of manufacturing activities

Estimation of the size of the lookup table

The data size of an alphanumeric digit in a text file is 1 byte (Eckstein, 2007).

Assuming that the lookup table is formed by five columns:

- Code – 4 digits reserved (4 bytes)
- Machine identifier – 50 digits reserved (50 bytes)
- Manufacturing facility – 100 digits reserved (100 bytes)
- Country of origin – 40 digits reserved (40 bytes)
- Status – 20 digits reserved (20 bytes)

The result is a maximum of 214 digits per record.

The total capacity of the table is related to the maximum number of combinations generated by a four-digit code, which is 1.68 million different combinations.

Consequently, the maximum data size of the table is estimated to be 359Mb.

However, considering a more realistic approximation, the size of the lookup table is reduced:

- Number of records: 183,952 (estimated number of manufacturing machines + distributors)
- Code: 4 digits
- Machine identifier: estimated average of 20 digits
- Manufacturing facility: estimated average of 60 digits
- Country of origin: estimated average of 10 digits
- Status: estimated average of 10 digits

In this case, a more realistic table size is estimated at 19.13Mb.

** Disclaimer: Digits reserved per element of information are based on assumptions.*

2.1.1.4.2. Product identification

In order to assess the formation of the code that represents the product identification as part of the UID, the following considerations were made:

- The global identification numbers such as GLN or GAIA (GS1, GS1 General Specifications, 2017) cannot be used (as a sub-part of the unique identifier code) because they introduce an excessive number of digits.
- To ensure the correct identification of the code by any approved equipment (even in offline mode), the information should be contained in a downloadable lookup table, which links the code to the product description of tobacco products.

Code length estimation

7,700 distinct product descriptions have been identified in the Spanish market (CMT, 2017). Therefore, in order to estimate the number of distinct products available in the EU market, the following assumption is made:

- The number of products available for consumption in each Member State is similar and the variety of products is completely distinct.

As a result, the estimation of the maximum number of distinct products identified in the EU market is 215,600.

A four-digit alphanumeric code can contain 1.68 million records, which is sufficient to encode all the product references (12.8% of the total capacity).

Element ID	Information requested	Code example	Number of characters
ID06	Product description	C3D4	4

Table 6: Example of code for unit packet identification

The following table shows an example of the lookup table layout, where the product description column includes the information requested by the TPD. Additionally, two extra columns include the product identifier (this can be an identification number such as GTIN) and the status (e.g. approved, pending approval, inactive or rejected) of the records.

Code	Product Description	Product Identifier	Status
H6D1	ABCDEF – 80gr	05153138484139	Approved
DLQ8	AT124 – 20 cigarettes	46839467319457	Pending approval

Table 7: Example of lookup table for product description

Estimation of the size of the lookup table

The data size of an alphanumeric digit in a text file is 1 byte.

Assuming that the lookup table is formed by two columns:

- Code – 4 digits reserved (4 bytes)
- Product description – 100 digits reserved (100 bytes)
- Product identifier – 20 digits reserved (20 bytes)
- Status – 20 digits reserved (20 bytes)

This results in a maximum of 144 digits per record.

The total capacity of the table is related to the maximum number of combinations generated by a four-digit code, which is 1.68 million different combinations.

Thus, the maximum data size of the table is estimated to be 242Mb.

However, considering a more realistic approximation, the size of the lookup table can be reduced:

- Number of records: 215,600 (estimated number of product identifiers in the EU)
- Code: 4 digits
- Product description: estimated average of 25 digits
- Product identifier: estimated average of 15 digits
- Status: estimated average of 10 digits

Therefore, a more realistic data size of the table is estimated to be 11.64Mb.

** Disclaimer: Digits reserved per element of information are based on assumptions.*

2.1.1.4.3. Date and time of the manufacturing activities

The date and time of the manufacturing activities group is composed of two elements:

- Date of manufacture
- Production shift or time of manufacture

In order to assess the formation of the code that represents the date and time of manufacturing activities as part of the UID, the following considerations were made:

- Dates and times are widely encoded under the following layout “YYMMDD” and “hhmmss”, where six numeric digits are used.
- The system should not distinguish between time zones and should be based on Coordinated Universal Time (UTC).
- The code should contain information about the time of manufacture instead of the shift, because it includes less ambiguity and the information is easier to identify by the competent authorities.
- The use of hours will be sufficient to reflect the time of manufacturing. This can be codified by using numeric digits, which avoids the use of lookup tables.

The manufacturing timestamp group is encoded into a single numeric 8-digit code presenting the information in “YYMMDDhh” format, representing the manufacturing timestamp. The last two digits can also correspond to the production shift.

Element ID	Information requested	Code example	Number of characters
ID01	Date of manufacture	21043013	8
ID05	Time of manufacture or production shift		

Table 8: Example of code for manufacturing timestamp

2.1.1.4.4. Shipment route information

The shipment route information group is formed of two elements:

- Intended market of sale
- Intended shipment route

In order to assess the formation of the code that represents the shipment route information as part of the UID, the following considerations were made:

- The intended shipment route is thought of as the list of countries that the unit packet will transit before reaching the intended market of sale, which is considered to be the last country on the list. Therefore, these two data elements may be combined in the same code.
- The shipment route can be encoded in an alphanumeric code.

- Due to supply chain complexity for the distribution of tobacco products, the addition of the entire shipping route will be restricted, because that information may not be known when production starts. Therefore, in order to provide more flexibility to the solution, it could be envisioned that the code will only reflect the first destination country of the shipment route.
- To ensure the correct identification of a code by any approved equipment (even in offline mode), it should be contained in a downloadable lookup table, which links the code to the information of the intended shipment route and the intended market of sale.

Estimation of the code length

The capacity of the code must contain all the possible routes for a net of 29 nodes (UE28 + Out of EU), with repetition allowed. The maximum number of combinations is calculated by the following formula:

$$\text{Maximum combinations} = n^2$$

There have been 841 possible routes identified between countries in the EU28 and the “out of EU” identifier.

A two-digit alphanumeric code can contain 1,296 records (65% over the total capacity). However, this capacity may be exceeded in the future. Therefore, our recommendation is a three-digit alphanumeric code that can contain 46,656 records, providing enough capacity to contain identifiers for every country in the world.

Accordingly, one independent code of three alphanumeric digits can be used to contain the information regarding the shipment route information in the unique identifier.

Element ID	Information requested	Code example	Number of characters
ID07	Intended market of retail sale	L2M	3
ID08	Intended shipment route		

Table 9: Example of code for shipment route information

The following table shows an example of the lookup table layout, where the columns *shipment route* and *intended market of sale* include the information requested by the TPD.

Code	Shipment route	Intended market of sale
G21	DE	ES
5H2	PO	Out of EU

Table 10: Example of lookup table for shipment route

Estimation of the size of the lookup table

The data size of an alphanumeric digit in a text file is 1 byte.

Assuming that the lookup table is formed by four columns:

- Code – 3 digits reserved (3 bytes)
- Intended shipment route – 20 digits reserved (20 bytes)
- Intended market of sale – 20 digits reserved (20 bytes)

This results in a maximum of 43 digits per record.

The total capacity of the table is related to the maximum number of combinations available (46,656).

Thus the maximum data size of the table is estimated to be 2Mb.

However, considering a more realistic approximation, the size of the lookup table is reduced:

- Number of records: 841 (estimated number of different routes)
- Code: 3 digits
- Intended shipment route: estimated average of 10 digits
- Intended market of sale: estimated average of 10 digits

Therefore, a more realistic data size of the table is estimated to be 19.3Kb.

** Disclaimer: Digits reserved per element of information are based on assumptions.*

2.1.1.4.5. Importer into the European Union

This group is composed of a single element: the importer into the European Union (only in such cases where the unit packet has been manufactured outside of the EU).

In order to assess the formation of the code that represents the importer into the European Union as part of the UID, the following considerations were reviewed:

- EORI (“Economic Operators Registration and Identification”) (TAXUD, 2009) is the number that identifies the economic operators that plan to import goods from countries outside the EU. However, its encoding is not considered because it introduces an excessive number of digits (12).
- The importer into the EU can be encoded in an alphanumeric code that covers all possibilities.
- To ensure the correct identification of a code by any approved equipment (even in offline mode), it should be contained in a downloadable lookup table, which links the code to the detailed information of the importer into the EU.
- If the unit packet has been manufactured within EU territory, this code will not provide information of any importer into EU territory, thus not altering the defined syntax.

Estimation of the code length

2,459 importers have been identified in the EU (Tobacco1, 2017).

A three-digit alphanumeric code can contain 46,656 records, which is sufficient to encode all the importers (6% over the total capacity).

One independent code of three alphanumeric digits can be used to contain the information regarding the importer into the EU in the unique identifier.

Element ID	Information requested	Code example	Number of
------------	-----------------------	--------------	-----------

			characters
ID09	Where applicable, the importer into the European Union	5P6	3

Table 11: Example of code for importer into the Union

The following table shows an example of the lookup table layout, where the importer column contains the information requested by the TPD. Additionally, two extra columns include the importer identifier (this can be an identification number such as EORI) and the status (e.g. approved, pending approval, inactive or rejected) of the records.

Code	Importer	Importer identifier	Status
G46	A1B2C Importer, Inc.	161384131	Approved
23S	DDEE Limited	598461365	Pending approval

Table 12: Example of lookup table for importers

Estimation of the size of the lookup table

The data size of an alphanumeric digit in a text file is 1 byte.

Assuming that the lookup table is formed by four columns:

- Code – 3 digits reserved (3 bytes)
- Importer – 100 digits reserved (100 bytes)
- Importer identifier – 20 digits reserved (20 bytes)
- Status – 20 digits reserved (20 bytes)

This results in a maximum of 126 digits per record.

The total capacity of the table is related to the maximum number of combinations generated by a three-digit code (46,656 combinations).

Thus the maximum data size of the table is estimated to be 6.71Mb.

However, considering a more realistic approximation, the size of the lookup table is reduced:

- Number of records: 2,800 (estimated number of importers)
- Code: 3 digits
- Importer: estimated average of 25 digits
- Importer Identifier: estimated average of 10 digits
- Status: estimated average of 10 digits

Therefore, a more realistic data size of the table is estimated to be 134Kb.

** Disclaimer: Digits reserved per element of information are based on assumptions.*

2.1.1.4.6. ID Issuer identification code

The ID Issuer is the entity responsible for the generation of the unique identifiers. Since multiple ID Issuer solutions may be established, an independent identification code should be used to identify them in order to avoid the duplication of serial numbers.

An independent alphanumeric two-digit code (with a capacity up to 1,296 registries) can be used to contain the information regarding the ID Issuer identification in the unique identifier.

Element ID	Information requested	Code example	Number of characters
ID10	ID Issuer	A3	2

Table 13: Example of ID Issuer identification code

2.1.1.4.7. Serial number

The serial number is the code that, when added to the rest of information elements, enables the unique identification of any unit packet. The serial numbers are generated by an ID Issuer upon the request of the manufacturers/importers.

- The uniqueness of the UID is provided by the combination of the serial number along with the rest of information requested by the TPD.
- In order to reduce its length, the uniqueness is achieved by the combination of several fields (ID Issuer identification code, place of manufacture, manufacturing facility, machine used to manufacture tobacco products, product description, intended market of retail sale, intended shipment route, importer into the EU and serial number), where the combination of these elements of information will always be unique. This permits a significant length reduction of the serial number while the flexibility of operations is maintained.
- As the information on date of manufacturing and time of manufacturing or production shift do not affect the uniqueness of the identifier, it may be added separately by manufacturers/importers in order to provide more flexibility.

Serial Number

The uniqueness of the UID code for any unit packet of tobacco products is achieved by combining the following elements:

- ID Issuer identification code
- Place of manufacture
- Manufacturing facility
- Machine used to manufacture the tobacco products
- Product description
- Intended market of retail sale
- Intended shipment route
- Importer into the EU
- Serial number



To ensure the uniqueness of the unique identifier, the serial number must provide enough capacity to encode production for a fixed timeline (assumed 100 years). This also provides flexibility to the manufacturers, who have the ability to request serial numbers from the ID Issuer in advance.

The following concepts have been reviewed in order to estimate the capacity of the code:

- Maximum production rate in high-speed production lines oscillates at about 1,000 unit packets per minute (1,440,000 unit packets per day).
- 365 days per year, in a 100-year timeline.
- The probability that the serial number can be guessed shall be negligible, and in any case will be lower than one in ten thousand (1:10,000).
- A multiplication factor of five is considered to account for the possible increase of production speed in the future.

A ten-digit alphanumeric code can contain $3.65 \cdot 10^{15}$ records, which is sufficient to encode all the produced units while maintaining the code's uniqueness.

Therefore, the serial number will be formed by a ten-digit alphanumeric code.

The following table illustrates the structure of the serial number.

Element ID	Information requested	Code example	Number of characters
ID11	Serial number	AAE5F26G7H	10

Table 14: Example of code for serial number

2.1.1.5. Summary of coding format for unique identifier

The main assumptions considered throughout the analysis are listed below:

- The global identification numbers such as GLN or GAIA (GS1, GS1 General Specifications, 2017) cannot be used (as a sub-part of the unique identifier code) because they introduce an excessive number of digits. The proposed data elements have been sized to accommodate exclusively the information needed according to the specific tracking and tracing sizing needs (e.g. quantity of manufacturing lines, quantity of products, quantity of potential shipment routes, etc.). In the particular case of the product identifier, its lookup table includes an optional column to refer to GTIN.
- According to the nature of the information, some data elements required by the TPD are grouped into one individual data element:

- The “Location of the manufacturing activities” element groups the following TPD data elements: place of manufacture, manufacturing facility and machine used to manufacture the tobacco products.
- The “Shipment route information” element groups the following TPD data elements: intended market for retail sale and intended shipment route. As before, a single code can comprise information from both data fields.
- Several elements are encoded by using alphanumeric characters in order to reduce code’s length.
- The calculation of the capacity of any data element includes a security margin of approximately 90%.

Finally, the study proposes a unique identifier structure composed of four elements of information:

- **ID Issuer identification code.**
 - The identification code of the independent ID Issuer responsible for providing the serial numbers.
- **Serial number**, generated by an independent ID Issuer.
 - The combination of the primary information, ID Issuer identification code and the serial number guarantees the code’s uniqueness for each unit packet.
- **Primary information**, required by the ID Issuer from the manufacturer or importer.
 - Formed by seven data elements: place of manufacture, manufacturing facility, machine used to manufacture the tobacco products, product description, intended market of retail sale, intended shipment route and importer into the EU.
- **Secondary information**, included by the manufacturer.
 - Formed by one element of information: the manufacturing timestamp, combining the date of manufacture and the time of manufacture or production shift.

Element ID	Information requested	TPD Reference	Code example	Length estimation
UID_1 <i>ID Issuer identification</i>	ID Issuer identification		A3	2
UID_2 <i>Serial number</i>	Serial number		AAE5F46G7H	10
UID_3 <i>Primary information</i>	Place of manufacture	Art 15(2)(a)	A1B2C3D4L2M3N4	14
	Manufacturing facility	Art 15(2)(b)		
	Machine used to manufacture the tobacco products	Art 15(2)(c)		
	Product description	Art 15(2)(e)		

Element ID	Information requested	TPD Reference	Code example	Length estimation
	Intended market of retail sale	Art 15(2)(f)		
	Intended shipment route	Art 15(2)(g)		
	Where applicable, the importer into the EU	Art 15(2)(h)		
UID_4 <i>Secondary information</i>	Manufacturing timestamp (Date of manufacture and time of manufacture or production shift)	Art 15(2)(a) Art 15(2)(d)	21043013	8
Total				34

Table 15: Coding format of the unique identifier at a unit packet level

Some of the data elements presented in the previous table require the establishment of lookup tables. The following table summarises the required lookup tables and their size.

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

Table 16: Summary of the lookup table's size

2.1.2. Requirements specification

After conducting the study of the unique identifier coding format, the following requirement specifications have been identified.

2.1.2.1. Functional

Functional Requirements – Tracking and Tracing – Unique identifier (at unit packet level)		
ID	Name	Priority
RQ_TTUU_FU_1	Data elements of the unique identifier	Must have
The unique identifier shall be composed of the following data elements: <ul style="list-style-type: none"> • the ID Issuer identification code; • a serial number; • the place of manufacturing; • the manufacturing facility; • the machine used to manufacture the tobacco products; • the product description; • the intended market of retail sale; • the intended shipment route; • where applicable, the importer into the EU; • the manufacturing timestamp combining the date of manufacturing and the time of manufacture or 		

Functional Requirements – Tracking and Tracing – Unique identifier (at unit packet level)		
ID	Name	Priority
	production shift.	
Source: Article 15(3) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		

2.1.2.2. Technical

2.1.2.2.1. System constraints

Technical Requirements – Tracking and Tracing – Unique identifier (at unit packet level)		
ID	Name	Priority
RQ_TTUU_SC_1	Uniqueness of the unique identifier	Must have
<p>The character sequence resulting from the combination of the manufacturing date, manufacturing machine and the serial number sequence should be unique.</p> <p>In order to avoid potential ambiguities and authentication errors, no unique identifiers having the same manufacturing date, manufacturing machine and serial number should be present in the Tracking and Tracing System at the same time.</p> <p>Source: Article 15(1) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)</p>		
RQ_TTUU_SC_2	Data element coding	Must have
<p>The structure of the unique identifier shall follow a predefined and well-known data syntax and semantics that allows the identification and accurate decoding of each data element of which the unique identifier is composed, using common scanning equipment.</p> <p>Source: Article 5(4) of (Commission Delegated Regulation (EU) 2016/161 - FMD, 2015)</p>		
RQ_TTUU_SC_3	Data element separators	Must have
<p>The coding scheme of the unique identifier shall include data identifiers or data qualifiers or other character sequences identifying the beginning and the end of the sequence of each individual data element of the unique identifier and defining the information contained in those data elements.</p> <p>Source: Article 5(4) of (Commission Delegated Regulation (EU) 2016/161 - FMD, 2015)</p>		
RQ_TTUU_SC_4	Unique identifier coding format	Must have
<p>The coding format of the unique identifier shall follow the rules described in section 2.1.1.5.</p> <p>Source: Section 2.1.1.5</p>		
RQ_TTUU_SC_5	Serial number format	Must have
<p>The serial number shall be a numeric or alphanumeric sequence of maximum 20 characters.</p> <p>Source: Contractor's expertise</p>		
RQ_TTUU_SC_6	Probability of serial number guessing	Must have

Technical Requirements – Tracking and Tracing – Unique identifier (at unit packet level)		
ID	Name	Priority
The probability that the serial number can be guessed shall be negligible and in any case lower than one in ten thousand. For that purpose, the generator of serial numbers could rely on randomisation techniques.		
Source: Article 4(c) of (Commission Delegated Regulation (EU) 2016/161 - FMD, 2015)		

2.1.2.3. Applicable Standards

Applicable Standards – Tracking and Tracing – Unique identifier (at unit packet level)		
ID	Name	Priority
RQ_TTUU_AS_1	Permissible character set of the identifier	Must have
The encoding of the identifier shall use alphabetic, numeric and special characters from the invariant character set ISO/IEC 646.		
Source: Part 3 of (ISO/IEC 15459:2014 - Unique identification, 2014)		

2.2. Unique identifier (at aggregation packaging level)

2.2.1. Assessment of the requirements and composition of the unique identifier

This section introduces the coding format proposed for the data elements that shall form part of the unique identifier at aggregation packaging level.

The Article 15(5) of the TPD sets out that the traceability requirements may be complied with by the marking and recording of aggregation packages such as cartons, master cases or pallets. Aggregation packages should be marked with a unique identifier. The creation of the unique identifier implies certain challenges:

- **Length of the unique identifier.** 1D data carriers are widely used in distribution chain operations. In order to be able to use the highest number of data carriers, the length of the unique identifier should not exceed a certain number of characters.
- **Access to readable information** for competent authorities. As stated, readable information is necessary to maximise the potential of the competent authorities to reduce illicit trade.
- **Similarity with unit packet unique identifier.** The use of previously created groups for the unique identifier at unit packet level restricts the complexity of the system and enables use of the lookup tables for the identification of both unit packet and aggregation packaging.

The analysis uses the following two-stage methodological approach:



Figure 6: Methodological approach for the codification of the unique identifier at aggregation packaging level

The following goals have been established for each stage respectively:

- Information analysis. This stage aims at identifying different attributes that qualify and categorise the information.
- Sizing optimisation. This stage aims at analysing different coding alternatives in order to optimise the sizing of the individual groups.

2.2.1.1. Baseline

The aggregation packages should be marked with a unique identifier to facilitate the activities of the Tracking and Tracing System. This enables increasing the operational efficiency while reducing costs in the supply chain (i.e., by marking a pallet with a unique identifier that contains 6,000 unit packets the distributor only needs to scan the receipt of the pallet's unique identifier, instead of scanning 6,000 unit packets).

In order to do so:

- The identification of the aggregation packages must be unique.
- In order to use the unique identifier to trade products along the supply chain, the unique identifiers must be linked with the unique identifiers of the elements contained inside.

Furthermore, the use of lookup tables is needed to decode the information contained in the unique identifier, while reducing its length.

2.2.1.2. Information analysis

The purpose is to identify the different groups of information that assure the uniqueness of the unique identifier and provide all the required information for the correct functioning of the Tracking and Tracing System.

This report suggests the use of these four groups in the composition of the unique identifier for aggregation packaging levels.

The following four elements of information form the unique identifier:

- Location of aggregation activities
- Date and time of aggregation activities
- ID Issuer identification code
- Serial number

2.2.1.3. Sizing optimisation

2.2.1.3.1. Location of the aggregation activities

The location of the aggregation activities group is formed by two elements:

- Location of aggregation activities
- Manufacturing or distribution facility

In order to assess the formation of the code that represents the location of the aggregation activities as part of the UID, the following considerations were made:

- The length of the code is envisioned to be equal to the code presented in section 2.1.1.4.1 for location of the manufacturing activities, so the same lookup table can be used to identify the location of the aggregation activities.
- It is envisioned to use only one code to encode the aggregation activities taking place in a manufacturing facility, which enables grouping the production coming from different production lines under a single code.

Estimation of the code length

It is estimated that there are approximately 332 tobacco manufacturing facilities in the EU, containing 743 production lines and 7,690 distribution facilities (everis, 2017). By assuming that consumption of tobacco products in the EU represents the 8.4% of the global consumption, the following assumptions are made:

- As consumption in the EU is 8.4% of the total, this percentage also represents the number of EU manufacturing and distribution facilities of the total in the world.
- Not all the facilities in the world will provide tobacco products to the EU.

The resulting estimation of the maximum number of facilities that could provide tobacco products to EU is 95,500 (manufacturing facilities within and outside the EU + distribution facilities within the EU).

By using a four-digit alphanumeric code, as proposed for unique identifier at unit packet level, the capacity of the code is 1.68 million records.

Assuming that all of these production lines can send tobacco products to the EU, the capacity of the code must be higher than the total number of facilities.

A four-digit alphanumeric code can contain 1.68 million records, which is sufficient to encode all the facilities and production lines (unique identifier at unit packet level) in the code (5.68% over the total capacity).

An independent four-digit alphanumeric code can be used to contain all the information needed to encode the location of aggregation activities in the unique identifier of the aggregation packaging levels.

Information provided	Code example	Number of characters
Place of aggregation	HK6H	4
Facility		

Table 17: Example of location of aggregation activities code

The lookup table used to decode the information is the same as that used for the location of manufacturing activities for the identification of the unit packet unique identifier. However, some columns are not filled because the information is not applicable to the aggregation activities (machine identifier).

Code	Machine Identifier	Manufacturing/Distribution Facility	Country of origin	Status
L40D	-	Industries 1A2B, Inc. ABC street, number 4, Madrid, Spain, zip code 28045	Spain	Approved
4H64	-	Industries 5Q84, Inc. RTY street, number 78, Lyon, France, zip code 69123	France	Pending of Approval

Table 18: Example of lookup table for location of aggregation activities

2.2.1.3.2. Date and time of aggregation activities

The coding format of the date of aggregation activities follows the next considerations:

- The code is composed of two elements: date and hour of aggregation to increase the flexibility of the operations.
- Dates and times are widely encoded under the following layout “YYMMDD” and “HHMMSS”, where six numeric digits are used.
- The system should not distinguish between time zones and should be based on Coordinated Universal Time (UTC).
- The use of hours will be sufficient to reflect the time of aggregation. This can be codified by using numeric digits, which avoids the use of lookup tables.

The two elements, date of aggregation and time of aggregation, are combined into a single 8-digit code presenting the information in the following format “YYMMDDhh”.

Information provided	Code example	Number of characters
Date of aggregation	21043013	8
Time of aggregation		

Table 19: Example of code for date and time of aggregation activities

2.2.1.3.3. ID Issuer identification code

The ID Issuer is the entity responsible for the generation of the unique identifiers. Since multiple ID Issuer solutions may be established, an independent identification code should be used to identify them in order to avoid the duplication of serial numbers.

An independent alphanumeric two-digit code (with a capacity up to 1,296 registries) can be used to contain the information regarding the ID Issuer identification in the unique identifier.

Information provided	Code example	Number of characters
ID Issuer	A3	2

Table 20: Example ID Issuer identification code

2.2.1.3.4. Serial number

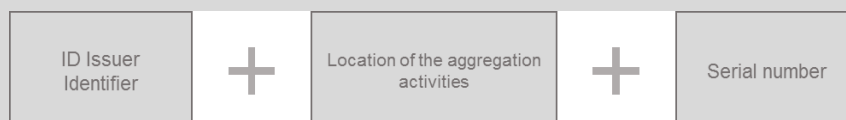
The serial number is the code that, when added to the rest of information elements, enables the unique identification of any unit packet. The serial numbers are generated by an ID Issuer upon the request of the manufacturers/importers.

- The uniqueness of the UID is provided by the combination of the serial number along with other data elements.
- In order to reduce its length, the uniqueness is achieved by the combination of several fields (ID Issuer identification code, location of aggregation activities and serial number), where the combination of these elements will always be unique. This permits a significant length reduction of the serial number while the flexibility of operations is maintained.
- As the information on date and time of aggregation do not affect the uniqueness of the identifier, it may be added separately by manufacturers/importers in order to provide more flexibility..

Serial Number

The uniqueness of the UID code for any unit packet of tobacco products is achieved by combining the following elements of information:

- ID Issuer identification code
- Location of manufacturing activities
- Serial number



To ensure the uniqueness of the unique identifier the serial number must provide enough capacity to encode production for a fixed timeline (assumed 100 years).

This also provides flexibility to the manufacturers, who have the ability to request serial numbers from the ID Issuer in advance.

The following concepts have been reviewed in order to estimate the capacity of the code:

- Maximum production rate in high-speed production lines oscillates at about 1,000 unit packets per minute (1,440,000 unit packets per day).
- 365 days per year, in a 100-year timeline.
- The probability that the serial number can be guessed shall be negligible, and in any case will be lower than one in ten thousand (1:10,000).
- A multiplication factor of five is considered to account for the possible increase of production speed in the future.

A ten-digit alphanumeric code can contain $3.65 \cdot 10^{15}$ records, which is sufficient to encode all the produced units while maintaining the code's uniqueness.

Therefore, the serial number will be formed by a ten-digit alphanumeric code.

The following table illustrates the structure of the serial number.

Information provided	Code example	Number of characters
Serial number	T03K55E322	10

Table 21: Example of code for serial number

2.2.1.4. Summary

The main assumptions considered in the analysis were the following:

- The unique identifier tries to use some data elements presented in the UID at unit packet level.
- Several elements are encoded by using alphanumeric characters in order to reduce code's length.

Finally, the study proposes a unique identifier at aggregation packaging structure composed of four elements of information:

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

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

Table 22: Example of location of manufacturing activities code

Moreover, one data element presented in the previous table required the establishment of lookup tables. As previously mentioned, these lookup tables are used for both unit packet level and aggregation packaging level. The following table summarises the lookup tables needed and their size.

Information requested	Realistic size	Maximum size
Location of the manufacturing or aggregation activities	19.13Mb	359Mb

Table 23: Summary of the lookup tables size

2.2.2. Requirements specification

After conducting the study of the unique identifier coding format, the following requirement specifications are identified.

2.2.2.1. Functional

Functional Requirements – Tracking and Tracing – Unique Identifier (at aggregation packaging level)		
ID	Name	Priority
RQ_TTUA_FU_1	Data elements of the unique identifier	Must have
The unique identifier shall be formed by the following data elements: <ul style="list-style-type: none"> the date of manufacturing the location of the aggregation activities the ID Issuer identification code a serial number 		
Source: Section 2.2.1		

2.2.2.2. Technical

2.2.2.2.1. System constraints

Technical Requirements – Tracking and Tracing – Unique identifier (at aggregation packaging level)		
ID	Name	Priority
RQ_TTUA_SC_1	Uniqueness of the unique identifier	Must have
The unique identifier shall be a sequence of numeric or alphanumeric characters that is unique to a given aggregation package of tobacco products.		
Source: Article 15(5) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTUA_SC_2	Data elements coding	Must have

Technical Requirements – Tracking and Tracing – Unique identifier (at aggregation packaging level)		
ID	Name	Priority
The structure of the unique identifier shall follow predefined and well-known data syntax and semantics that allows the identification and accurate decoding of each data element of which the unique identifier is composed, using common scanning equipment.		
Source: Article 5(4) of (Commission Delegated Regulation (EU) 2016/161 - FMD, 2015)		
RQ_TTUA_SC_3	Data elements separators	Must have
The coding scheme of the unique identifier shall include data identifiers or data qualifiers or other character sequences identifying the beginning and the end of the sequence of each individual data element of the unique identifier and defining the information contained in those data elements.		
Source: Article 5(4) of (Commission Delegated Regulation (EU) 2016/161 - FMD, 2015)		
RQ_TTUA_SC_4	Unique identifier coding format	Must have
The coding format of the unique identifier shall follow the rules described in section 2.1 of this Annex		
Source: Annex II – Section 2.1		
RQ_TTUA_SC_5	Serial number format	Must have
The serial number shall be a numeric or alphanumeric sequence of maximum 20 characters.		
Source: Article 4(b)(ii) of (Commission Delegated Regulation (EU) 2016/161 - FMD, 2015)		
RQ_TTUA_SC_6	Probability of serial number guessing	Must have
The probability that the serial number can be guessed shall be negligible and in any case lower than one in ten thousand. For that purpose, the number generation could rely on randomisation techniques.		
Source: Article 4(c) of (Commission Delegated Regulation (EU) 2016/161 - FMD, 2015)		

2.2.2.3. Applicable standards

Applicable Standards – Tracking and Tracing – Unique identifier (at aggregation packaging level)		
ID	Name	Priority
RQ_TTUA_AS_1	Permissible character set of the identifier	Must have
The encoding of the identifier shall use alphabetic, numeric and special characters from the invariant character set ISO/IEC 646.		
Source: Part 3 of (ISO/IEC 15459:2014 - Unique identification, 2014)		

2.3. Data carrier (at unit packet level)

2.3.1. Preliminary analysis


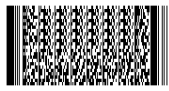

The purpose of the preliminary analysis is to identify the competitive landscape of those data carriers that could include the unique identifier without negatively affecting operations.

- The data carrier allows encoding alphanumeric digits.
- The maximum number of characters enabled in the data carrier is higher than the current length of the unique identifier (34 characters).
- The data carrier is not restricted to specific industries or organisations.
- The code represents specifically a data carrier symbology.
- The data carrier is already implemented in the operations of manufacturers, importers and distributors.

2.3.1.1. Data carrier competitive landscape

The review of the competitive landscape identifies a multitude of data carrier types, clustered into the five categories listed in the table below.

The purpose of this analysis is to identify the wide variety of data carriers utilised in different operational areas. Thus, it is possible to select the most suitable data carrier to meet the requirements previously stated.

Categories of data carriers		
Linear 1D Data Carriers	<p>Description:</p> <ul style="list-style-type: none"> • Linear barcodes encode the information in one direction, which is stored in the relationship of the bar widths between each other. • In most of these symbologies the height of the bar is not relevant, except for some height modulated Postal Codes. 	
	<p>Types:</p> <p>Bookland, Codabar, Code 11, Code 2 of 5, Code 2 of 7, Code 25, Code 32, DAFT, DOD Logmars, DUN-14, DUNS, EAN, FIN Code, Flattenmarken, Code 128, HIBC, ISBN, ISBT, ISMN, ISSN, ITF-14, JAN, MSI, NVE-18, NW-7, Pharmacode, Plessey Code, Rational Codebar, SCC-14, SSCC-18, Telepen, UPC, USD-4, Postal Codes, Code 39, Code 93, VIN Code.</p>	
2D Data Carriers Stacked	<p>Description:</p> <ul style="list-style-type: none"> • The 2D Data Carriers (Stacked) are multi-row barcodes, storing the information in two dimensions. In order to do so, several linear stacked barcodes are used to encode the information. 	
	<p>Types:</p> <p>Codablock, MicroPDF417, PDF417.</p>	
2D Data Carriers (Matrix Codes)	<p>Description:</p> <ul style="list-style-type: none"> • The 2D Data Carriers encode the information in two dimensions. The encoding of the information is based on the position of the black (or white) dots, differing from 2D Data Carriers (Stacked) that encode the information using different bar widths. 	



Categories of data carriers		
	Types: Aztec Code, Data Matrix, DotCode, Han Xin Code, MaxiCode, MicroQR, QR Code.	
Composite Codes	Description: <ul style="list-style-type: none"> The Composite Codes combine linear and two dimensional symbologies. This combination enables encoding the most important information in the linear barcode, whereas the additional data can be stored in the 2D component. This separation ensures better migration (e.g. with respect to scanning hardware) between linear and 2D technology. 	
	Types: GS1 Composite Symbologies.	
Electronic Data Carriers	Description: <ul style="list-style-type: none"> The electronic data carriers use electromagnetic fields to transmit the encoded information. Unlike the data carriers previously presented, the tag does not need to be within the line of sight of the reader, so it may be embedded in the tracked object. 	
	(2) Types: RFID, NFC, Beacons.	
(3) Sources: (TEC-IT, 2017) (GS1, GS1 General Specifications, 2017) (Sciences, 2015)		

Table 24: Categories of data carriers

2.3.1.2. Preliminary selection of data carriers

The review of the competitive landscape in the previous section has identified the set of data carrier types available on the market. However, not all of them are suitable to hold the unique identifier.

The preliminary selection of the data carriers is based on the following selection criteria:

- The data carrier allows encoding alphanumeric digits.
- The maximum number of enabled characters is higher than 30 digits, which is the estimated length for the unique identifier.
- The use of the data carrier is not restricted to specific industries or organisations.
- The code specifically represents a data carrier symbology.

The result of the preliminary filtering outlines that 11 types of data carriers fulfil the four selection criteria presented above. These types of data carrier are: Code 128, Code 39, Code 93, Aztec Code, Codablock, Data Matrix, DotCode, Han Xin Code, MaxiCode, PDF417 and QR Code.

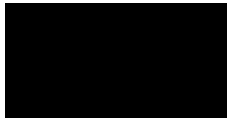


Nevertheless, as this report aims at designing a solution to be further implemented in the supply chain of tobacco products in Europe, the selected data carrier should not present a significant burden for the stakeholders. In order to mitigate its effect, an additional selection criterion is added, which dictates that the data carrier should already be implemented in manufacturing and distribution operations. The following table presents

the most used data carriers in the industry and their applications (Priyanka Gaur, 2014) (GS1, GS1 Barcode Fact Sheet, 2015) (TEC-IT, 2017) (University, 2011) (Cognex, 2013).

Data Carrier	Typical Usage
Code 128	Extensively used worldwide in shipping and packaging as product identification
Code 39	Postal services
Code 93	Canada postal service
Aztec code	Transport, governmental, commercial
Codablock	Used for small labels and secure data, HIBC
Data Matrix	Aerospace, Components, U.S. Mail, Pharma, Tobacco Industry, HIBC, Defence, & Printed Media
DotCode	High speed marking for food, tobacco and pharmaceutical products
Han Xin Code	Logistic activities in Asia
MaxiCode	Logistic activities in US
PDF417	Airline industry, identification cards
QR Code	Automotive, commercial tracking applications

Table 25: Typical usage of data carriers

A list of six types of data carriers has been created for further analysis. This preliminary list includes the following data carriers:

Data Carrier	Description	Example
Code 128	<ul style="list-style-type: none"> • 1-Dimensional data carrier. • It can encode all 128 characters of ASCII. • The symbology is defined as ISO/IEC 15417:2007. 	
Aztec Code	<ul style="list-style-type: none"> • 2-Dimensional data carrier. • All 8-bit values can be encoded. • It has the potential to use less space than other matrix barcodes. • The symbology is defined as ISO/IEC 24778:2008. 	
Data Matrix	<ul style="list-style-type: none"> • 2-Dimensional data carrier. • It can encode the entire ASCII character set. • It can include up to 2,335 alphanumeric characters. • The symbology is defined as ISO/IEC 16022:2006. 	



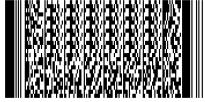












Data Carrier	Description	Example
DotCode	<ul style="list-style-type: none"> • 2-Dimensional data carrier. • It can encode ASCII characters. • It is ideally suited for high speed industrial ink jet and laser marking techniques. • DotCode symbology specifications are defined by AIM. 	
QR	<ul style="list-style-type: none"> • 2-Dimensional data carrier. • It can encode the entire ASCII character set. • It can include up to 4,296 alphanumeric characters. • The symbology is defined as ISO/IEC 18004:2006. 	
PDF417	<ul style="list-style-type: none"> • It is a stacked linear data carrier. • It can encode all 128 characters of ASCII. • The symbology is defined as ISO/IEC 15438:2006. 	

Table 26: Preliminary selection of data carriers

2.3.2. Analysis for the selection of data carriers

The purpose of this analysis is to indicate the data carrier or group of data carriers that best fulfils the needs of each product category (clustered by production speed and product type), based on evaluation parameters. The scoring for each data carrier varies linearly from non-compliant to fully compliant with each evaluation parameter.

Category 1: cigarettes in high-speed production lines

Evaluation Parameter	Aztec Code	Code 128	Data Matrix	DotCode	PDF417	QR Code	Comments
Technical feasibility							Sources: <ul style="list-style-type: none"> • Solution providers consultation • Manufacturers consultation
	Comments: <ul style="list-style-type: none"> • All the presented data carriers, except Code 128, are able to be printed or affixed in all types of cigarette unit packets. • Two printing technologies, continuous ink jet and laser, permit printing DotCode at a high-speed rate over 1,000 ppm. • DotCode printing equipment is already implemented in a number of high-speed production lines, according to the manufacturers during the stakeholders consultation. • In the stakeholders consultation, solution providers pointed out DotCode as the only data carrier able to be printed at high-speed rate. • Distribution operations usually deal with aggregation packages of cigarettes, therefore they do not have to scan the products at unit packet level. • The ISO standard 15415:2011 (Information technology – Automatic identification and data capture techniques – Bar code symbol print quality test specification – Two-dimensional symbols) specifies two methodologies for the measurement of specific attributes of two-dimensional bar code symbols. 						
Operational requirements							Sources: <ul style="list-style-type: none"> • Solution providers' consultation • Manufacturers' consultation

Evaluation Parameter	Aztec Code	Code 128	Data Matrix	DotCode	PDF417	QR Code	Comments
							<p>Comments:</p> <ul style="list-style-type: none"> • DotCode printing equipment is implemented in a number of manufacturing facilities, which benefits its further implementation in more production lines due to the acquired expertise. • DotCode is the only data carrier that can be printed at the required pace per production line, while not affecting production. • The stakeholders consultation also highlights that DotCode can be verified at production line speed. • The other selected data carriers are not able to be printed at manufacturing production rate.
Burden for stakeholders							<p>Sources:</p> <ul style="list-style-type: none"> • Solution providers consultation • Manufacturers consultation <p>Comments:</p> <ul style="list-style-type: none"> • Continuous ink jet and laser printing technologies incur a significant burden for the stakeholders. • The burden in DotCode printers is lower since a number of production lines are already equipped with this technology. • Additionally, verification equipment should be implemented in production lines.

Table 27: Data carriers analysis for Category 1 of tobacco products

Category 2: cigarettes in low/medium-speed production lines

Evaluation Parameter	Aztec Code	Code 128	Data Matrix	DotCode	PDF417	QR Code	Comments
Technical feasibility							<p>Sources:</p> <ul style="list-style-type: none"> • Solution providers consultation • Manufacturers consultation <p>Comments:</p> <ul style="list-style-type: none"> • All the presented data carriers, except Code 128, are able to be printed or affixed in all unit packets of cigarettes. • A wider range of printing technologies are able to print at low/medium speed to meet production demands, which enables a larger range of data carriers to be printed (Aztec, QR Code, Data Matrix, DotCode). • The stakeholders consultation reveals that only DotCode is currently printed in cigarette manufacturing. • At low/medium production speed the data carriers are also able to be affixed in the unit packet. • The ISO standard 15415:2011 (Information technology – Automatic identification and data capture techniques – Bar code symbol print quality test specification – Two-dimensional symbols) specifies two methodologies for the measurement of specific attributes of two-dimensional barcode symbols.
Operational requirements							<p>Sources:</p> <ul style="list-style-type: none"> • Solution providers consultation • Manufacturers consultation <p>Comments:</p> <ul style="list-style-type: none"> • DotCode printing equipment is implemented in a number of manufacturing facilities, which benefits its further implementation in more production lines due to the acquired expertise. • Data Matrix is the most extended data carrier in traceability solutions, which is transmitted in different specialised equipment available on the market. • All the selected data carriers can be printed and verified at the designated production speed.
Burden for stakeholders							<p>Sources:</p> <ul style="list-style-type: none"> • Solution providers consultation • Manufacturers consultation <p>Comments:</p> <ul style="list-style-type: none"> • Continuous ink jet and laser printing technologies incur a significant burden for stakeholders. • The burden in DotCode printers is lower since a number of production lines are already equipped with this technology. • Printing and verifying equipment of Data Matrix is already installed in a variety of production facilities. • In addition to printers, verification equipment should be included in production lines.

Table 28: Data carriers analysis for Category 2 of tobacco products

Category 3: other tobacco products in high-speed production lines

Evaluation Parameter	Aztec Code	Code 128	Data Matrix	DotCode	PDF417	QR Code	Comments
Technical feasibility							Sources: providers <ul style="list-style-type: none"> • Solution consultation • Manufacturers consultation
	Comments: <ul style="list-style-type: none"> • All the presented data carriers are able to be printed or affixed in all the tobacco product sizes presented in the stakeholders consultation. • Two printing technologies, continuous ink jet and laser, permit printing DotCode at a high-speed rate over 1,000 ppm. • DotCode printing equipment is already implemented in a number of high-speed production lines, according to the manufacturers consultation. • Distribution operations usually deal with aggregation packages of other tobacco products rather than cigarettes; therefore, they do not have to scan the products at unit packet level. • Solution providers consultation points out DotCode as the data carrier able to be printed at high-speed rate for other tobacco products. • In some cases, the printing rate may be affected by the material of the tobacco products. • The ISO standard 15415:2011 (Information technology – Automatic identification and data capture techniques – Bar code symbol print quality test specification – Two-dimensional symbols) specifies two methodologies for the measurement of specific attributes of two-dimensional bar. 						
Operational requirements							Sources: providers <ul style="list-style-type: none"> • Solution consultation • Manufacturers consultation
	Comments: <ul style="list-style-type: none"> • DotCode printing equipment is implemented in a number of manufacturing facilities, which benefit the further implementation in more production lines due to the acquired expertise. • DotCode is the only data carrier that can be printed at the pace required per production line, while not affecting the production pace. • The stakeholders consultation also highlights that DotCode can be verified at production line speed. • The rest of the selected data carriers are not able to be printed at manufacturing production rate 						
Burden for stakeholders							Sources: providers <ul style="list-style-type: none"> • Solution consultation • Manufacturers consultation
	Comments: <ul style="list-style-type: none"> • Continuous ink jet and laser printing technologies incur a significant burden for the stakeholders. • The burden in DotCode printers is lower since a number of production lines are already equipped with this technology. • Additionally, verification equipment should be implemented in production lines. 						

Table 29: Data carriers analysis for Category 3 of tobacco products

Category 4: other tobacco products in low/medium-speed production lines

Evaluation Parameter	Aztec Code	Code 128	Data Matrix	DotCode	PDF417	QR Code	Comments
Technical feasibility							Sources: providers <ul style="list-style-type: none"> • Solution consultation • Manufacturers consultation
	Comments: <ul style="list-style-type: none"> • All the presented data carriers are able to be printed or affixed in all the tobacco product sizes presented in the stakeholders consultation. • A wider range of printing technologies are able to print at low/medium-speed to meet production demands, which enables a larger range of data carriers to be printed (Aztec, QR Code, Data Matrix, DotCode). • The stakeholders consultation reveals that Data Matrix is currently printed in the manufacturing of other tobacco products rather than cigarettes. • Distribution operations usually deal with aggregation packages, therefore they do not have to scan the products at unit packet level. • In some cases, the printing rate may be affected by the packaging material. • The ISO standard 15415:2011 (Information technology – Automatic identification and data capture techniques – Bar code symbol print quality test specification – Two-dimensional symbols) specifies two methodologies for the measurement of specific attributes of two-dimensional barcodes. 						













Evaluation Parameter	Aztec Code	Code 128	Data Matrix	DotCode	PDF417	QR Code	Comments
Operational requirements							Sources: <ul style="list-style-type: none"> • Solution consultation providers • Manufacturers consultation
	Comments: <ul style="list-style-type: none"> • All the data carriers can be printed at the established production speed. • Data Matrix and Code 128 printing equipment are installed in a number of manufacturing facilities for traceability purposes (Data matrix) and logistics purposes (Code 128). 						
Burden for stakeholders							Sources: <ul style="list-style-type: none"> • Solution consultation providers • Manufacturers consultation
	Comments: <ul style="list-style-type: none"> • Continuous ink jet and laser printing technologies incur a significant burden for the stakeholders. • Most of the data carriers symbologies can be implemented in production lines without excessive cost. • The burden in Data Matrix printers is lower since a number of production lines are already equipped with this technology. • Additionally, verification equipment should be implemented in production lines. 						

Table 30: Data carriers analysis for Category 4 of tobacco products

Allowed data carriers

The objective of the criteria analysis was to select the type of data carrier that best suits the needs of each of the categories highlighted. After conducting the analysis, three data carriers - Data Matrix, DotCode and QR - were found to be best suited to encoding the unique identifier at unit packet level.

It is therefore recommended that each unit packet of any tobacco product be marked with one of the above-mentioned data carriers. The following table sets out their main characteristics.



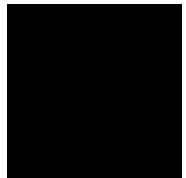
Data Carrier	Characteristics	Example
Data Matrix	<ul style="list-style-type: none"> • Able to be printed by multiple technologies either directly on the package or on a label to later be affixed. • Currently used in the marking of other tobacco products other than cigarettes. 	
DotCode	<ul style="list-style-type: none"> • Able to be printed in high-speed production lines through continuous ink jet or laser printing technologies. • Currently used at unit packet level by several tobacco manufacturers. 	
QR	<ul style="list-style-type: none"> • Able to be printed by multiple technologies either directly on the package or on a label to later be affixed. • It is one of the most used data carriers worldwide and compatible with multiple scanning solutions. 	

Table 31: Allowed data carriers for unit packet of tobacco products

2.3.3. Technical requirements

The TPD requires all the unit packets of tobacco products to be marked with a unique identifier. This requirement can be fulfilled through the following:

- All the unit packets of tobacco products must include a data carrier that contains the unique identifier.
- The data carrier at unit packet level must be one of the following: Data Matrix, DotCode, or QR.

2.4. Data carrier (at aggregation packaging level)

2.4.1. Analysis for the selection of data carriers

The purpose of this analysis was to indicate the data carrier or group of data carriers that best fulfil the needs of each product category, clustered by aggregation level and based on evaluation parameters.

Category 1: aggregation level 1, carton or bundle.

Evaluation Parameter	Aztec Code	Code 128	Data Matrix	DotCode	PDF417	QR Code	Comments
Technical feasibility							Sources: • Solution providers consultation • Manufacturers consultation • Distribution chain operators consultation
	Comments: <ul style="list-style-type: none"> • The aggregation packaging does not represent space problems to include the data carriers that contain the unique identifier. • Production speeds at aggregation packaging are significantly lower than at unit packet level, which permits implementing a wider range of printing technologies. • Production speed and aggregation packaging material influence the printing or affixing process. • The stakeholders consultation reveals that Data Matrix and Code 128 are currently printed in the aggregation packaging of tobacco products for traceability purposes. • Wholesalers usually deal with laser and image scanners, which enable the identification of 1D and 2D data carriers respectively. 						
Operational requirements							Sources: • Solution providers consultation • Manufacturers consultation • Distribution chain operators consultation
	Comments: <ul style="list-style-type: none"> • All the data carriers can be printed at the established production speed. • Data Matrix and Code 128 printing equipment are installed in a number of manufacturing facilities for traceability purposes (Data Matrix) and logistics purposes (Code 128). • The stakeholders' consultation reveals that distribution chain operators are equipped to read both 1D and 2D barcodes. 						
Burden for stakeholders							Sources: • Solution providers consultation • Manufacturers consultation • Distribution chain operators consultation
	Comments: <ul style="list-style-type: none"> • Most of the data carriers symbologies can be implemented in production line without excessive cost. • The burden for Data Matrix and Code 128 printers is lower since a number of production lines are already equipped with this technology. • Additionally, verification equipment should be implemented in production lines. 						

Table 32: Data carriers analysis for Category 1 of aggregation packaging

Category 2, aggregation level 2, shipping case.



















Evaluation Parameter	Aztec Code	Code 128	Data Matrix	DotCode	PDF417	QR Code	Comments
Technical feasibility							Sources: <ul style="list-style-type: none"> • Solution providers consultation • Manufacturers consultation • Distribution chain operators consultation • (GS1, GS1 Identification Keys in Transport & Logistics, 2013)
	Comments: <ul style="list-style-type: none"> • The aggregation packaging level 2 (shipping case) does not represent space problems to include the data carriers that contain the unique identifier. • Production speeds are lower than aggregation packaging level 1, reducing problems of printing speed. • Stakeholders consultation shows that most manufacturers use Code 128 and Data Matrix affixed to the shipping case. • Code 128 is the most used symbology in logistics operations. • 1D barcodes are the most used by distribution chain operators in logistic activities. 						
Operational requirements							Sources: <ul style="list-style-type: none"> • Solution providers consultation • Manufacturers consultation • Distribution chain operators consultation
	Comments: <ul style="list-style-type: none"> • All the data carriers can be printed or affixed at the established production speed. • Data Matrix and Code 128 printing equipment are installed in a number of manufacturing facilities. • The stakeholders consultation reveals that distribution chain operators use 1D barcodes and laser scanners for logistic purposes. 						
Burden for stakeholders							Sources: <ul style="list-style-type: none"> • Solution providers consultation • Manufacturers consultation • Distribution chain operators consultation
	Comments: <ul style="list-style-type: none"> • The burden for Data Matrix and Code 128 printers is lower since a number of production lines are already equipped with this technology. • The burden for scanning equipment is reduced if Code 128 is selected, due to the extensive use of laser scanners. 						

Table 33: Data carriers analysis for Category 2 of aggregation packaging

Allowed data carriers

After conducting the analysis, three data carriers – Data Matrix, Code 128 and QR– were found to be best suited to encoding the unique identifier at aggregation packaging level.

It is therefore recommended that each aggregation packaging level of tobacco products be marked with at least one of the above-mentioned data carriers. The following table sets out their main characteristics.

Data Carrier	Characteristics	Example
--------------	-----------------	---------



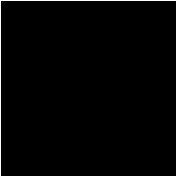
Data Carrier	Characteristics	Example
Data Matrix	<ul style="list-style-type: none"> • Able to be printed by multiple technologies, either directly on the package or on a label to later be affixed. • Currently used in the marking of aggregation packaging of tobacco products. 	
Code 128	<ul style="list-style-type: none"> • Widely used in logistics operations and able to be read by laser scanners. • Currently used in the marking of aggregation packaging of tobacco products. 	
QR	<ul style="list-style-type: none"> • Able to be printed by multiple technologies either directly on the package or on a label to later be affixed. • It is one of the most used data carriers worldwide and compatible with multiple scanning solutions. 	

Table 34: Allowed data carriers for aggregation packaging levels of tobacco products

The inclusion of additional data carriers that contain the unique identifier can facilitate the tracking and tracing activities of wholesalers and distributors is allowed.

2.4.2. Technical requirements

The Article 15(5) of the TPD sets out that the traceability requirements may be complied with by the marking and recording of aggregation packages such as cartons, master cases or pallets. This requirement could be fulfilled by complying with the following specifications:

- Aggregation packages of tobacco products eligible for traceability purposes are marked with at least one data carrier containing the unique identifier.
- The data carrier at aggregation packaging level must be at least one of the following: Data Matrix, Code 128 or QR.
- The optional addition of data carriers that contain the unique identifier is permitted to facilitate the tracking and tracing activities.

3. DETAILED TECHNICAL SPECIFICATIONS FOR THE IT ARTEFACTS OF THE TRACKING AND TRACING SYSTEM

3.1. System Architecture

This section provides an overview of the main conceptual elements and relationships of the System architecture, which will include subsystems, components, data stores, users and external systems.

Prior the architecture specification, the following analyses were conducted:

- **Requirements specification** (i.e. functional and non-functional) to clearly specify the capabilities and behaviour of the System and the priority of each feature.
- Identification of **goals** to be met in order to properly shape the final System.
- Description of general findings that allow relevant architectural **decisions** to be taken.

The System architecture described within this section is conceptual, which means that is independent of any technology or product. The technical details of the implementation of each element will be provided by the third party provider that establishes his/her specific solution as part of the System.

3.1.1. Requirements specification

The individual requirements of each component of the Tracking and Tracing System have been collected in the following sections:

- Unique identifier at unit packet level (see section 2.1.2)
- Unique identifier at aggregation packaging level (see section 2.2.2)
- System for the issuance of unique identifiers (see section 3.10.1)
- Temporary Buffer optional component (see section 3.4.1)
- Messaging events (see section 3.5.1)
- Primary Data Storage (see section 3.7.1)
- Surveillance Data Storage (see section 3.8.1)
- Repository Router (see section 3.9.1)

These requirements have driven the architecture described below.

3.1.2. Architectural goals

The goals that the architecture needs to be met are formulated below:

- **Simplicity.** The Tracking and Tracing System architecture shall promote simplicity and avoid unnecessary complexities. Whenever complexity is required, it must be encapsulated within re-usable components.

- **Modularity.** The Tracking and Tracing System architecture shall follow a modular approach, dividing the overall system into smaller sub-systems that are co-dependent but can be designed independently of each other. These sub-systems can interoperate by exchanging information through documented interfaces in order to provide the necessary functionality. Modular components increase the systems' capacities to adapt to different evolution needs, because any change is isolated from the other modules or sub-systems.
- **Technology independence.** The Tracking and Tracing System architecture shall be independent and neutral of any specific technology, commercial or open source product in order to be product and technology agnostic and avoid vendor locking.
- **Interoperability.** The Tracking and Tracing System interfaces and protocols shall be based on open standards to promote interoperability, reduce the impact of technological changes on economic operators, decouple from specific implementations and facilitate the integration processes.
- **Scalability.** The Tracking and Tracing System architecture shall support a sustainable growth in regard to the following: a) the volume and size of the events of tobacco products being reported; b) the number of economic operators reporting; and c) the number of competent authorities' systems extracting surveillance data (e.g. tax or customs national systems). Since there is no comparable EU-wide traceability system of such scale, the System must be able to gracefully support increasing amounts of workload.
- **Security.** The Tracking and Tracing System architecture shall ensure the following security principles: a) confidentiality (i.e. only allowing access to data for which the user has the right permissions); b) integrity (i.e. ensuring data is not tampered or altered by unauthorised users; and c) availability (i.e. ensuring that systems and data are available to authorised users when they need it).

3.1.3. Architectural decisions

This section describes the architectural decisions that were carefully considered prior to the architecture specification. These decisions evaluate the following issues:

- **Where** must the components to which the distributors and wholesalers are reporting (i.e. Repository Router) be physically located? There is no obvious answer for the following reasons:
 - The System must be connected to a number of distributors and wholesalers.
 - The Primary Data Storages are established per manufacturer or importer.
 - A report may refer to several importers or manufacturers.
- **What** is the best approach to exchange data with external systems that are not yet known? Some key users' systems have already been identified, namely ECMS and SEED, with whom communication could be made possible. However, the System shall be prepared to smoothly allow other external systems to communicate with it as well (e.g. client systems of the competent authorities, FCTC global information-sharing focal point, etc.).

3.1.3.1. Repository Router component established as a central component

Subject Area	Repository Router component	Topic	Distributed vs centralised topology
Architectural Decision	Repository Router shall be established as a central component within the Tracking and Tracing System	ID	AD-01
Issue or Problem Statement	The Tracking and Tracing System shall provide to the distributors and wholesalers a component (i.e. Repository Router) that seamlessly routes their events to the proper Primary Data Storage established by the manufacturers or importers referred to in the event. To this end, three alternatives are possible with regard to the router topology: a) it is established within the central Surveillance Data Storage; b) it is established as a distributed component within each Primary Data Storage; or c) it is established as a distributed component within the facilities of each economic operator that has to report.		
Assumptions	In order to properly route aggregation events, it is necessary to access the complete list of unique identifiers in order to know who has manufactured/imported the tobacco products referred to.		
Motivation	<p>This decision is important for the following reasons:</p> <ul style="list-style-type: none"> • The implementation complexity of the Repository Router depends on its final topology (i.e. centralised versus distributed). • The risk of having unrouteable events increases if the Repository Router is not able to know which manufacturer/importer must be informed about an aggregation event. This happens if the overall traceability information is not available for the Repository Router. 		
Alternatives	(See problem statement)		
Decision	The Repository Router shall be established as a central component within the Tracking and Tracing System.		

Justification	<p>The disadvantages of a distributed topology are as follows:</p> <ul style="list-style-type: none"> • A distributed router topology, at a Primary Data Storage level, would imply that any data received in a Repository Router must to be broadcasted to the other Repository Routers. Each Repository Router must decide if this data must be consolidated into its own repository or not. In order to make this decision, the router has a data dependency: the manufacturer/importer of the tobacco products of the aggregated IDs must be known. This data dependency always exists in any case, whether there is a central router or distributed routers. With a central router, the message routing is performed more efficiently (i.e. routing exclusively to the Primary Data Storage that must process the message). • With distributed routers, at a Primary Data Storage level, all the events are broadcasted. Thus, the amount of data to be stored globally and also for each individual distributed storage is multiplied by a large factor. • It is more difficult with distributed routers, at a Primary Data Storage level, to process aggregation events because a distributed router does not have the overall information regarding who must receive the message. Thus, in the particular case of events with unique identifiers that do not belong to a specific storage (i.e. manufacturer/importer), the distributed router must wait, and store these reports pending to be processed during a much longer period of time (i.e. final expiration time) to decide if these events must be removed from the pending messages. Therefore, it is most likely that many events will remain stored unnecessarily in repositories that will never route them because all the data from the distributors and wholesalers is broadcasted to all the routers, even if they do not own them. • In the case of distributed routers at a facility level, the complexity is moved down to the economic operators, which shall establish a router that should be aware of all the Primary Data Storages and should have enough information (i.e. unique identifiers and their manufacturer/importer). This alternative poses major maintenance and performance challenges taking into account the amount of UIDs managed by the system and that the Primary Data Storages' configuration shall be made available to thousands of routing components located at the facilities of the distributors and wholesalers. This would imply a big impact on integration and operation.
Implications	-
Derived requirements	See requirements of the Repository Router component.
Related Decisions	-

Table 35: Architectural decision - Repository Router

3.1.3.2. Usage of a canonical data model to exchange data with competent authorities and auditors

Subject Area	Canonical data model	Topic	Design pattern for integration
Architectural	The interfaces that exchange data with	ID	AD-02

Decision	competent authorities and auditors shall use a canonical data model
Issue or Problem Statement	<p>In order to facilitate full data access to competent authorities and auditors, it is necessary to use a standard approach that promotes interoperability and extensibility with new external systems that may have different data needs. These needs may evolve in the future. To this end, the possible alternatives are the following:</p> <ul style="list-style-type: none"> • Define a canonical data model that comprises the details of all the entities to be exchanged. • Find a workaround for the EPCIS standard to allow the exchange of unique identifiers not issued by GS1 and define a canonical data model for the rest of the information to be exchanged. • Use metadata to allow understanding which set of entities are exchanged.
Assumptions	<p>Firstly, there is no currently available standard data model that supports the exchange of all the data required by the TPD (i.e. tracking, tracing and trade). It should be noted that there is one standard that allows the exchange of supply chain event data, (ISO/IEC 19987:2015 EPCIS, 2016). However, this standard is meant to exchange only visibility event data related to GS1 identifiers and does not support some specific data that has to be managed by the System, inter alia: lookup data for UID decoding, notifications, and unique identifiers.</p> <p>Secondly, the canonical data model shall be used only for the data exchange with the competent authorities and the auditors, since these System users shall have full access to all relevant data, as required by the TPD.</p> <p>Finally, any other data exchange between the different solutions of the System shall follow the message specification (e.g. reports transmitted by economic operators, requests of issuance of serial numbers, etc.).</p>
Motivation	This decision is important to promote interoperability and facilitate full data access to the systems of competent authorities and auditors. It also facilitates integration with new systems (e.g. tax or custom national systems) whose data needs are not known at this stage.
Alternatives	(See problem statement)
Decision	Use a canonical data model to exchange data with competent authorities and auditors.
Justification	<p>Using of a canonical data model provides the following advantages:</p> <ul style="list-style-type: none"> • This is an accepted approach for logical data models in the absence of industry standards (F. Ferguson, Donald; Hadar, Ethan, 2012) (Supply Chain Insights, 2014). • It greatly normalises conceptual and logical data models. Thus, the domain specific knowledge required for the integration is not very high. • This data model is more explicit because data is described in great detail, listing all entities and relationships and specifying attributes for each entity. Therefore, it allows integration efforts to be reduced. Also, the interpretation errors are minimised. • This approach is a widely used integration pattern for exchanging domain specific data between applications that use different data formats. • It is an independent and abstract protocol that, for exchange purposes, could be mapped to different open standard data protocols such as XML (W3C XML, 2016) or JSON (ECMA 404 - JSON, 2013).
Implications	-

Derived requirements	-
Related Decisions	-

Table 36: Architectural decision – Canonical data model

3.1.4. Overview diagram

The overview diagram of the Tracking and Tracing System is depicted as follows:

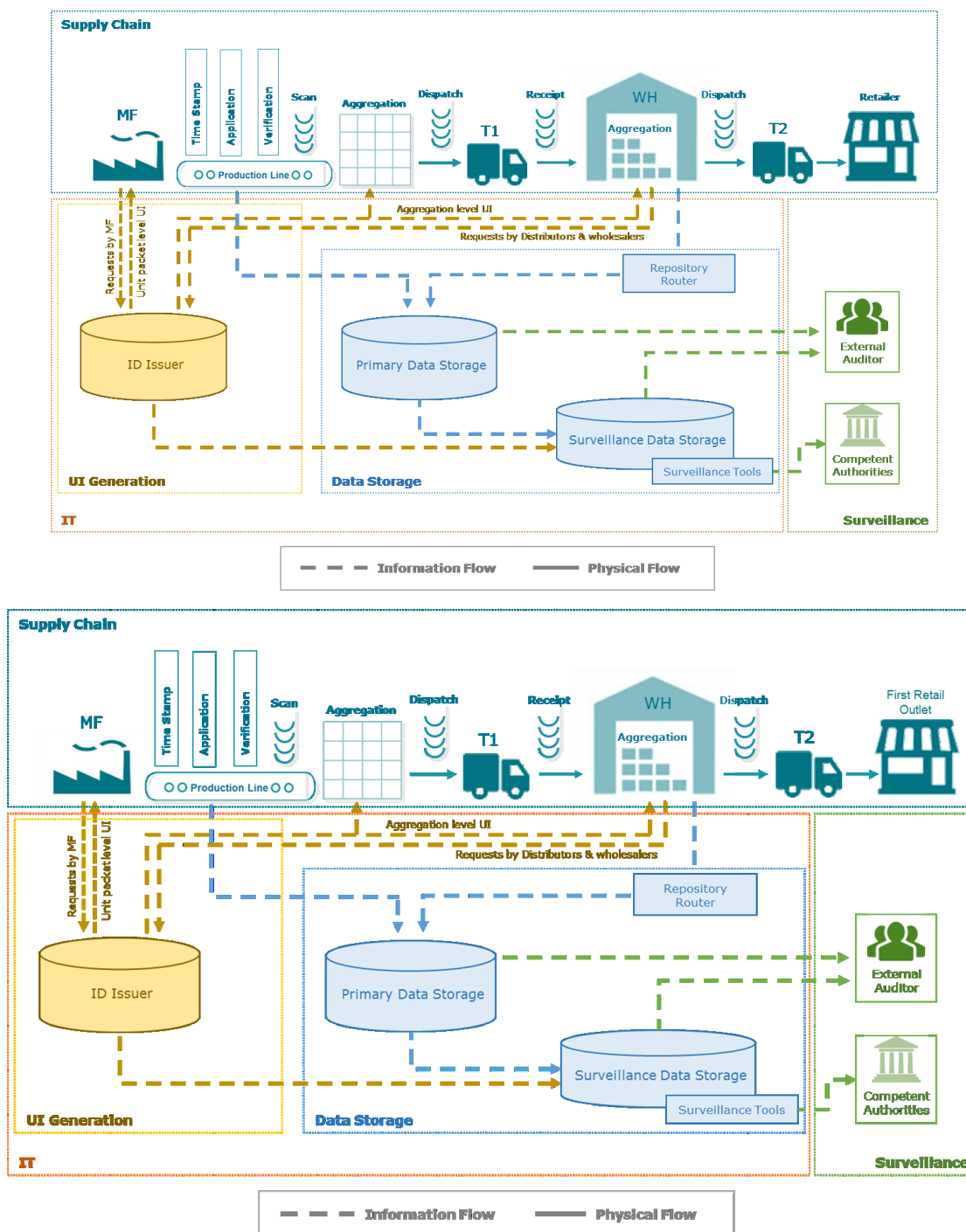


Figure 7: System overview diagram

The Tracking and Tracing System can be seen divided into three major conceptual domain groups, namely:

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

The Supply Chain domain encloses economic operators with their production and movement of tobacco products throughout the supply chain, and these events are reported to the Data Storages located at the Data Capture domain. The details of the processes of the Supply Chain domain are presented in the business process diagrams (Section 1.3 of this Annex).

Hence, the Tracking and Tracing System architecture comprises three layers of storage, namely:

- The **Temporary Buffer**, which is an optional component established on a voluntary basis by the economic operators at a facility level that reports events to the Tracking and Tracing System;
- A group of independent and decentralised **Primary Data Storage** solutions;
- A central **Surveillance Data Storage** solution.

The optional **Temporary Buffer** component can be established in the facilities of the economic operators, on a voluntary basis. This component is only responsible for **securely transmitting** the reports to the Tracking and Tracing System, as required by the TPD. This component is recommended because allows economic operators to decouple the reporting of events from the manufacturing and distribution activities and also mediates communication. The transmission of events is not required to be done in real time, nor do the production and logistic processes wait for a delivery acknowledge. This optional component should act as a **safety buffer** to temporarily hold data events as they are received, serving as a short-term assurance against any service interruption in the upper storage layer that is receiving the data stream. If the delivery of events is not correctly acknowledged, the reporting component should re-try again the transmission of these events.

The optional Temporary Buffer is expected to contain a local interface to collect the information from the on-site systems and devices (e.g. production lines, scanners, etc.) that has to be transmitted. It should be noted that the Temporary Buffer **does not manage the integration with the economic operators' legacy systems** because it is assumed that all the necessary information (e.g. trade data) has been collected previously.

The second layer of storage is a **group of independent Primary Data Storage solutions**, where each storage **hosts data exclusively related to a specific manufacturer or importer**. As required by the TPD, this data shall be transmitted by all the economic operators involved in the trade of tobacco products, from the manufacturer to the last economic operator before the first retail outlet, and refers to the following relevant transactions of tobacco products: entry into their possession, intermediate movements, and final exit from their possession. The Primary Data Storage solution shall

also support the reporting at aggregation packaging level in order to promote efficient communications, data processing and storage.

Each Primary Data Storage solution shall be established by an independent third party data storage provider, which must be appointed and contracted by each specific manufacturer or importer. The Commission is responsible for approving these contracts and the selected external auditor.

The third layer of storage is a central **Surveillance Data Storage solution** which hosts a **global copy** of the distributed data. On this basis, the Surveillance Data Storage solution is in a position to offer a **comprehensive logical view** of all relevant data from local data, which could be further exploited through analytic capabilities (e.g. risk based analytics, suspicious pattern detection, etc.) to increase the efficiency and effectiveness of national enforcement activities. Furthermore, this central Surveillance Data Storage solution provides a secure Repository Routing component to facilitate the seamless transmission of events reported by distributors and wholesalers through a single point. The Surveillance domain shown in Figure 7, [Figure 7: System overview diagram](#), involves competent authorities of Member States, the Commission, and auditors, which are the system users to access data for enforcement and combat the illicit trade of tobacco products. The details of some capabilities of this domain are presented in the Use Cases (Section 1.5 of this Annex).

In this particular case, the third party providers of the Primary Data Storage solutions would jointly select the third party data storage provider that will establish the Surveillance Data Storage solution.

In addition, the Primary Data Storage solution and the Surveillance Data Storage solution must contain standard and secure interfaces, which provide full access to the relevant tobacco products data to all parties authorised under the TPD.

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 of Member States 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 e) manufacturers and importers must 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 Primary Data Storage solution.

The System also comprises a group of **ID Issuer solutions** that generate the serial numbers required to assure the uniqueness of the unique identifiers. The purpose of the ID Issuer solution is threefold: a) provision of serial numbers to the economic operators for their activities; b) notify the central Surveillance Data Storage solution of which serial numbers have been provisioned. The System comprises one ID Issuer solution per Member State, who appoints the independent third party serial number provider that will establish the solution at a national level; and c) offer registration services to the economic operators. These registration services allow the population of lookup data needed for the unique identifier serialisation. The lookup registers are related to: economic operator, facility of manufacturing, and machine of manufacturing.

Finally, it should be pointed out that the **transmission of events** shall be done **within the time frame prescribed** by the Implementing Regulation.

The high-level system architecture of the Tracking and Tracing System is depicted as follows, based on the standard UML class diagram notation (ISO/IEC 19505-1:2012 UML, 2014):

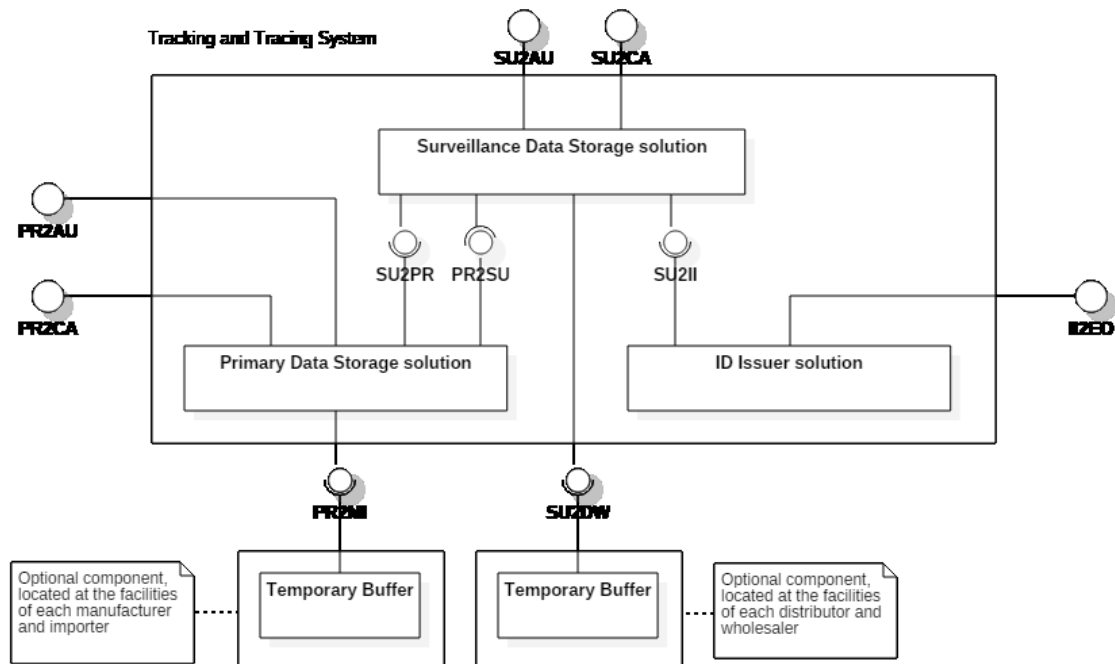


Figure 8: High-level system architecture diagram

The interfaces of the Tracking and Tracing System are as follows:

Interface acronym	Hosting system	Description
PR2MI	Primary Data Storage	Secure interface published to manufacturers and importers to acquire the messages reported from their facilities.
PR2CA	Primary Data Storage	Secure interface published to the competent authorities to allow full access to the data stored in this repository.
PR2AU	Primary Data Storage	Secured interface published to the auditors to allow access for auditing purposes of this repository.
PR2SU	Primary Data Storage	Secure interface published to the Surveillance solution to allow the exchange of messages routed by its Repository Router component and the replication of lookup tables. The Repository Router receives messages from the distributors and wholesalers but is only responsible for routing each message to the Primary Data Storage that shall process this information.
II2EO	ID Issuer solution	Secure interface published to the economic operators to request the generation of serial numbers, either at

		unit packet level or at aggregation packaging levels.
SU2DW	Surveillance Data Storage	Secure interface published to distributors and wholesalers to acquire the messages reported from their facilities.
SU2CA	Surveillance Data Storage	Secure interface published to the competent authorities to allow full access to the data stored in this repository. This also includes the lookup tables used for simplification of the encoding of the unique identifier.
SU2AU	Surveillance Data Storage	Secure interface published to the auditors to allow access for auditing purposes of this repository.
SU2PR	Surveillance Data Storage	Secure interface published to the Primary Data Storage solution to allow the copy of messages previously received at the Primary Data Storage.
SU2II	Surveillance Data Storage	Secure interface published to the ID Issuer solution to allow the notification of serial number generation.

Table 37: Tracking and Tracing System interfaces

It should be noted that each interface mentioned above may contain different physical endpoints. In this way, the final solution implementation is able to provide specialised access due to performance, logical data partitioning, or security reasons.

Finally, the medium-level system architecture of the Tracking and Tracing System is depicted below, based on the standard UML class diagram notation (ISO/IEC 19505-1:2012 UML, 2014):

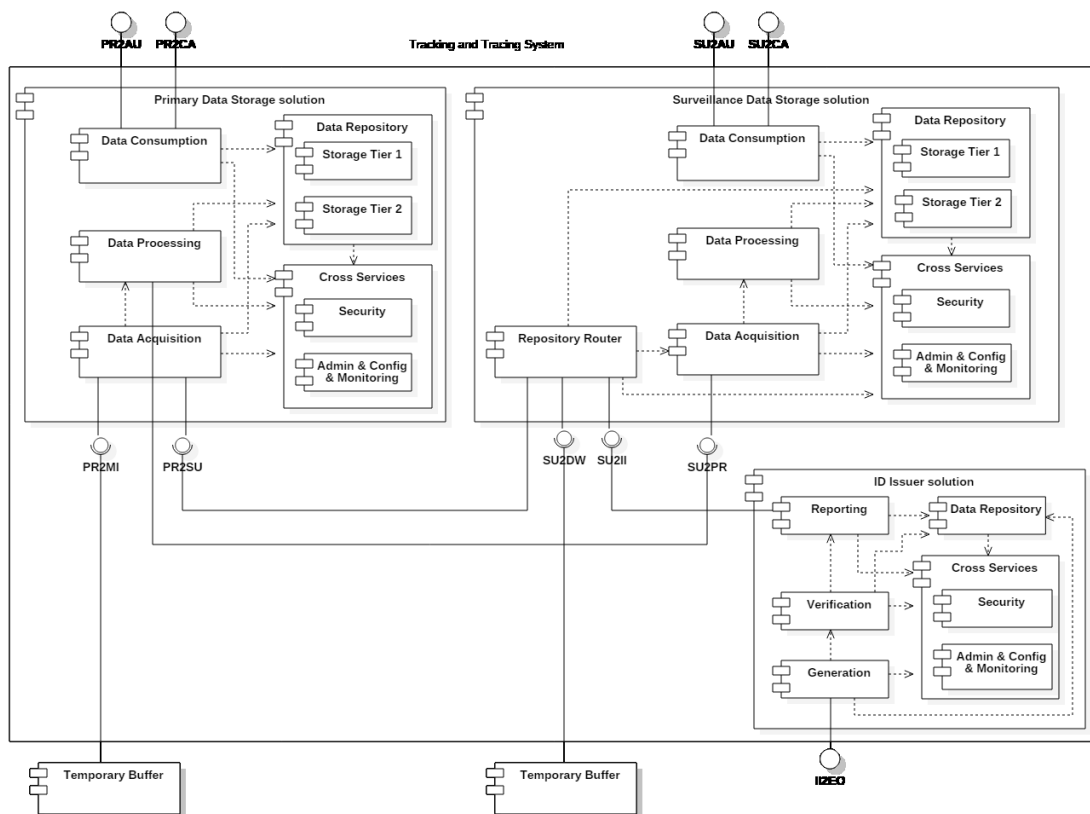
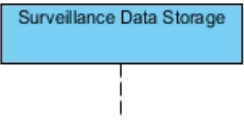

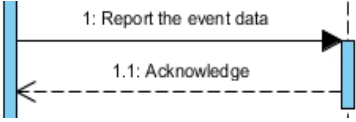
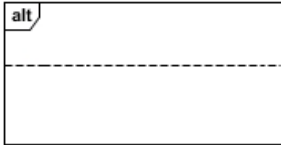
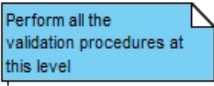


Figure 9: Medium-level components' architecture diagram

3.2. Sequence diagrams

This section shows the sequence diagram of the Tracking and Tracing System. This diagram is based on the business process diagrams and on the system architecture diagram. The sequence diagram shows the interactions between roles or objects in the sequential order that those interactions occur. The standard notation to illustrate the sequence diagram is UML (ISO/IEC 19505-1:2012 UML, 2014). This notation provides various symbols intended to explain the different objects that interact throughout the sequence.

	<p>Lifeline notation elements are placed across the top of the diagram. They are drawn as a box with a dashed line descending from the top down to the bottom. They represent either roles or object instances that participate in the sequence. The lifeline's name is placed inside the box.</p>
	<p>An actor symbol is a lifeline used to represent an external system's boundary entity.</p>
	<p>Incoming and outgoing messages (a.k.a. interactions) are represented by arrows connecting from the border of the</p>

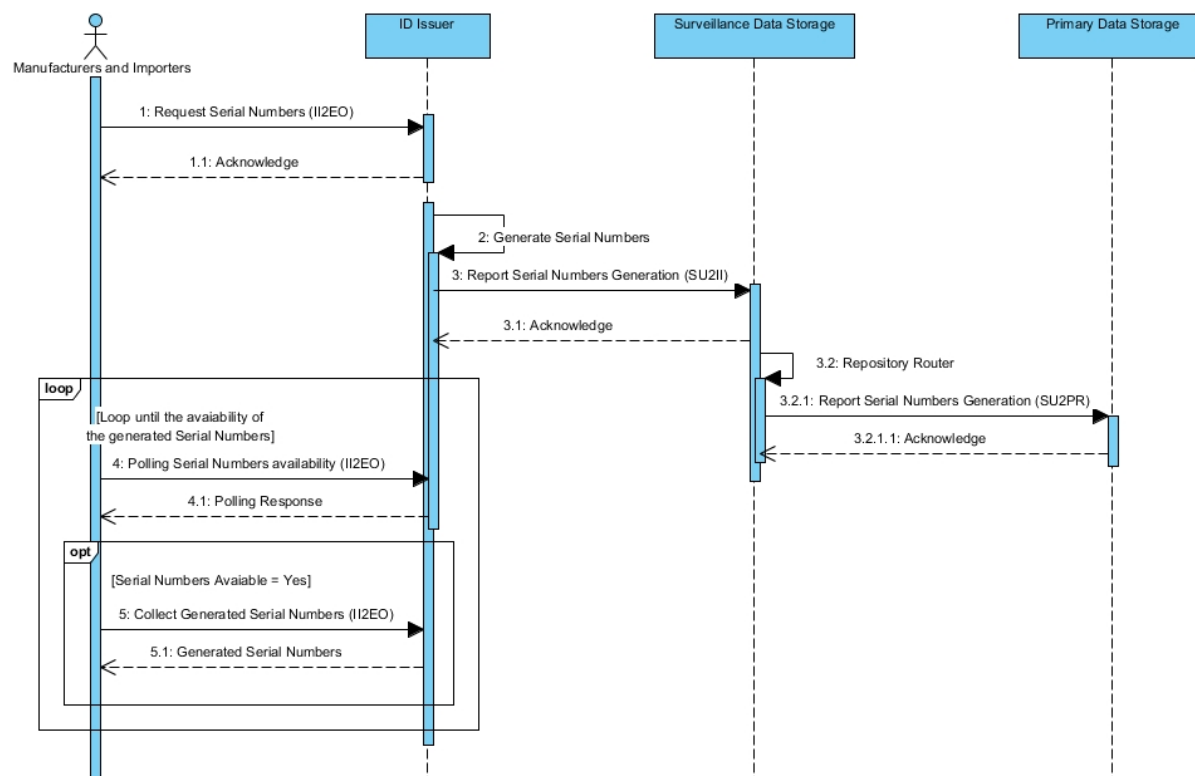
	<p>sender to the border of the receiver.</p> <p>The first message is typically located on the left side of the diagram for readability. Subsequent messages are then added to the diagram just below the previous message.</p> <p>To represent an object (lifeline) sending a message to another object, a line is drawn from the sender to the receiving object. The message name is placed above the arrowed line.</p> <p>Besides showing message calls on the Sequence Diagram, the interactions also may include return messages. A return message is drawn as a dotted line with an open arrowhead pointing back to the originating lifeline, and above this dotted line the return value from the operation.</p> <p>There are cases when an object needs to send a message to itself, which is represented by a connection of the message back to the object. By showing an object sending itself a message, the model highlights the fact that this processing takes place within the object.</p>
	<p>A frame element represents a consistent place providing a graphical boundary for the interaction. In addition to providing a visual border, the frame element has an important functional use in diagrams depicting interactions.</p> <p>In this diagram, four types of frames are used:</p> <p>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.</p> <p>opt: Options are used to designate a sequence that, given a certain condition, will occur. Otherwise, the sequence does not occur, allowing the model to represent the classic “if then” logic.</p> <p>loop: A loop sequencing fragment (denoted “loop”) encloses a series of messages which must be processed within a loop until the occurrence of a constraint.</p> <p>par: A parallel sequencing fragment (denoted “par”) encloses a series of messages which can be independently processed in parallel.</p>
	<p>Comments regarding the interaction, positioned next to the item referred to.</p>

3.2.1. Request for serial number

The sequence of a request for the generation of serial numbers.

3.2.1.1. Manufacturers and importers

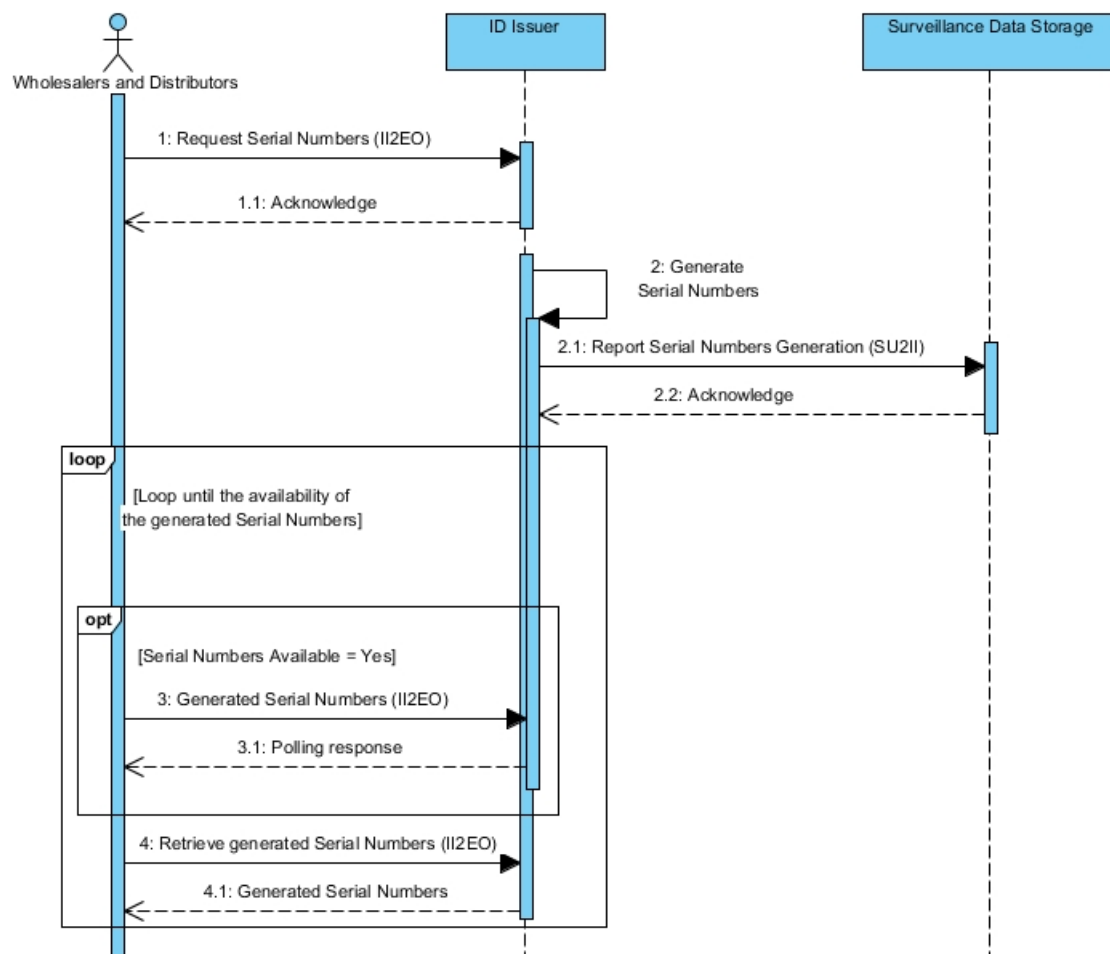
The diagram below depicts the sequence for serial number generation when requested by manufacturers and importers.



Sequence Description	
ID	Description
▪ 1	▪ Manufacturers and importers request the serial numbers generation from the ID Issuer using the II2EO interface
▪ 1.1	▪ ID issuer acknowledges reception of the request
▪ 2	▪ ID issuer generates the serial numbers
▪ 3	▪ ID issuer reports to the Surveillance Data Storage the generated serial numbers using the SU2II interface
▪ 3.1	▪ Surveillance Data Storage acknowledges reception of the message
▪ 3.2	▪ Surveillance Data Storage performs the data routing procedures through the Repository Router
▪ 3.2.1	▪ Surveillance Data Storage routes the issuance reporting to the correspondent Primary Data Storage using the SU2PR interface
▪ 3.2.1.1	▪ Primary Data Storage acknowledges reception of the message
▪ 4	▪ Manufacturers and importers check the serial numbers availability using the II2EO interface
▪ 4.1	▪ ID issuer responses the serial numbers availability
▪ 5	▪ Manufacturers and importers collect the serial numbers when eventually become available using the II2EO interface
▪ 5.1	▪ Manufacturers and importers receive the generated serial numbers

3.2.1.2. Wholesalers and distributors

The diagram below depicts the sequence for serial number generation requests made by wholesalers and distributors, which is slightly different from the sequence for the issuance of serial numbers for manufacturers and importers. As the issuance of serial numbers for wholesalers and distributors is used only for the identification of a variety of product aggregation levels, the data routing to the respective Primary Data Storages will occur when the wholesaler or distributor informs the usage of that issued serial number within the aggregation event report, where it is possible to identify the manufacturer or importer of the aggregated product and therefore, the respective Primary Data Storage.



Sequence Description	
ID	Description
▪ 1	▪ Wholesalers and distributors request the serial numbers generation from the ID Issuer using the II2EO interface
▪ 1.1	▪ ID issuer acknowledges reception of the request
▪ 2	▪ ID issuer generates the serial numbers
▪ 2.1	▪ ID issuer reports to the Surveillance Data Storage the generated serial numbers using the SU2II interface
▪ 2.2	▪ Surveillance Data Storage acknowledges reception of the message
▪ 3	▪ Wholesalers and distributors check the serial numbers availability using the II2EO interface

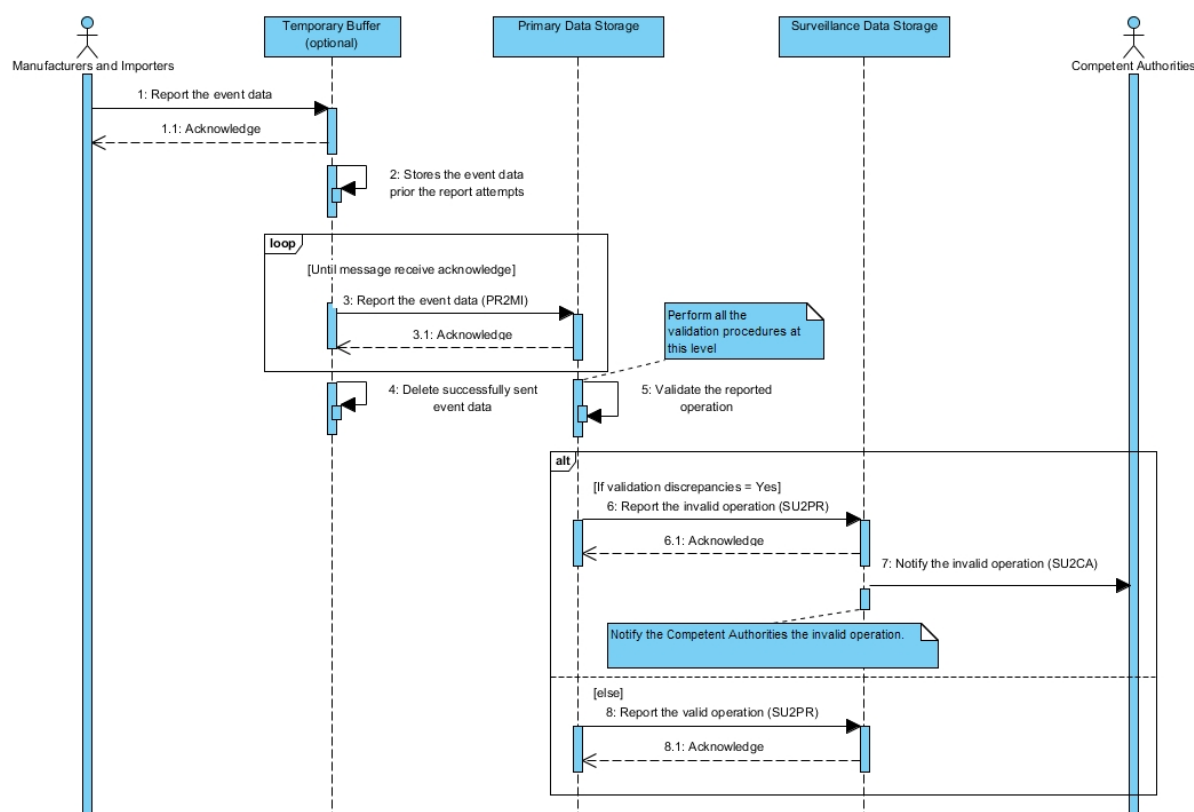
▪ 3.1	▪ ID issuer responds the serial numbers availability
▪ 4	▪ Wholesalers and distributors collect the serial numbers when eventually become available using the I12EO interface
▪ 4.1	▪ Wholesalers and distributors receive the generated serial numbers

3.2.2. Event reporting

The following sequence diagrams present the event reporting. This reporting is triggered when a relevant event occurs. The complete list of relevant reporting events is defined by the business processes. The sequence of the event reporting is slightly different when performed by manufacturers and importers than when performed by wholesalers and distributors, as depicted in the following diagrams.

3.2.2.1. Manufacturers and importers

The diagram below depicts the sequence of event reporting as performed by manufacturers and importers through the optional reporting component Temporary Buffer.

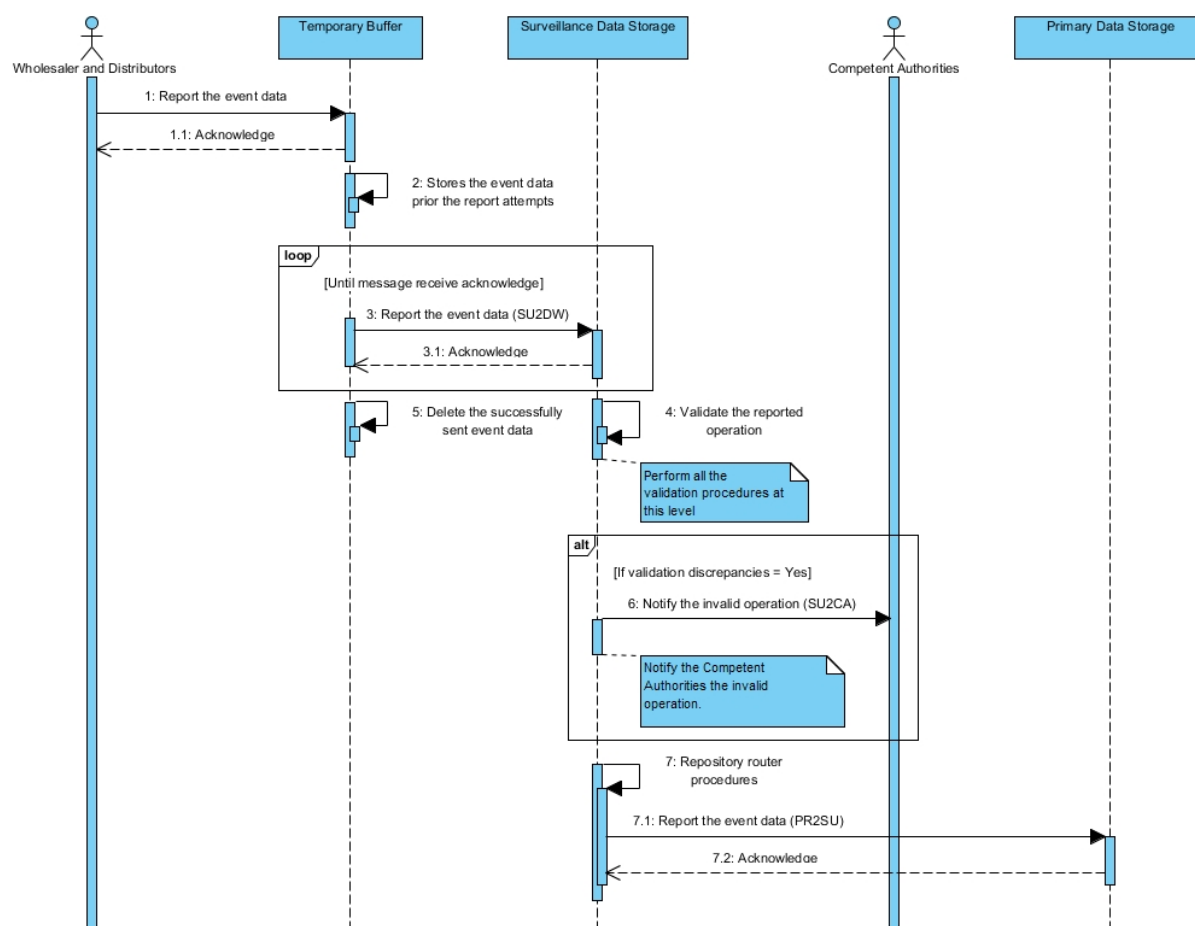


Sequence Description	
ID	Description
▪ 1	▪ Manufacturers and importers report the event data. Optionally, this reporting can be performed using the Temporary Buffer or directly to the Primary Data Storage using the PR2MI interface
▪ 1.1	▪ Temporary Buffer acknowledges reception of the report
▪ 2	▪ Temporary Buffer stores the event data collected prior to the attempt to report an

	event to the Primary Data Storage
▪ 3	▪ Temporary Buffer loops the attempt to send the event data to the Primary Data Storage using the PR2MI interface
▪ 3.1	▪ Primary Data Storage acknowledges reception of the message
▪ 4	▪ Optionally, the Temporary Buffer deletes the event data after the acknowledgement of the event data reception from the Primary Data Storage
▪ 5	▪ Primary Data Storage performs the event data validation process
▪ 6	▪ If discrepancies are found in the validation process, the Primary Data Storage reports the invalid operation to the Surveillance Data Storage using the SU2PR interface
▪ 6.1	▪ Surveillance Data Storage acknowledges reception of the message
▪ 7	▪ In case of discrepancies, the Surveillance Data Storage reports the invalid operation to the competent authorities using the SU2CA interface
▪ 8	▪ If no discrepancies are found in the validation process, the Primary Data Storage reports the valid operation to the Surveillance Data Storage using the SU2CA interface
▪ 8.1	▪ Surveillance Data Storage acknowledges reception of the message

3.2.2.2. Wholesalers and distributors

The diagram below depicts the sequence of event reporting as performed by wholesalers and distributors.



Sequence Description	
ID	Description

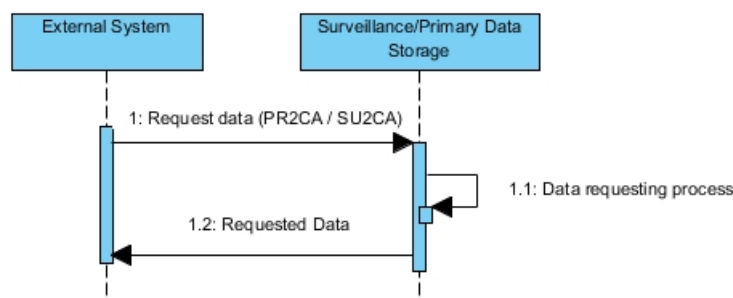
▪ 1	▪ Wholesalers and distributors report the event data
▪ 1.1	▪ Temporary Buffer acknowledges reception of the report. Optionally, this reporting can be performed using the Temporary Buffer or directly to the Surveillance Data Storage using the SU2DW interface
▪ 2	▪ Temporary Buffer stores the event data collected prior to the attempt to report an event to the Surveillance Data Storage
▪ 3	▪ Temporary Buffer loops the attempt to send the event data to the Surveillance Data Storage using the SU2DW interface
▪ 3.1	▪ Surveillance Data Storage acknowledges reception of the message
▪ 4	▪ Surveillance Data Storage performs the event data validation process
▪ 5	▪ Optionally, the Temporary Buffer deletes the event data after the acknowledgement of the event data reception from the Surveillance Data Storage
▪ 6	▪ If discrepancies are found in the validation process, the Surveillance Data Storage reports the invalid operation to the competent authorities using the SU2CA interface
▪ 7	▪ Surveillance Data Storage performs the data routing procedures
▪ 7.1	▪ Surveillance Data Storage routes the event data to the correspondent Primary Data Storages using the PR2SU interface
▪ 7.2	▪ Primary Data Storages acknowledge the data reception

3.2.3. Data outbound

The following diagrams depict the sequence for data reading processes by external systems.

3.2.3.1. Synchronous request

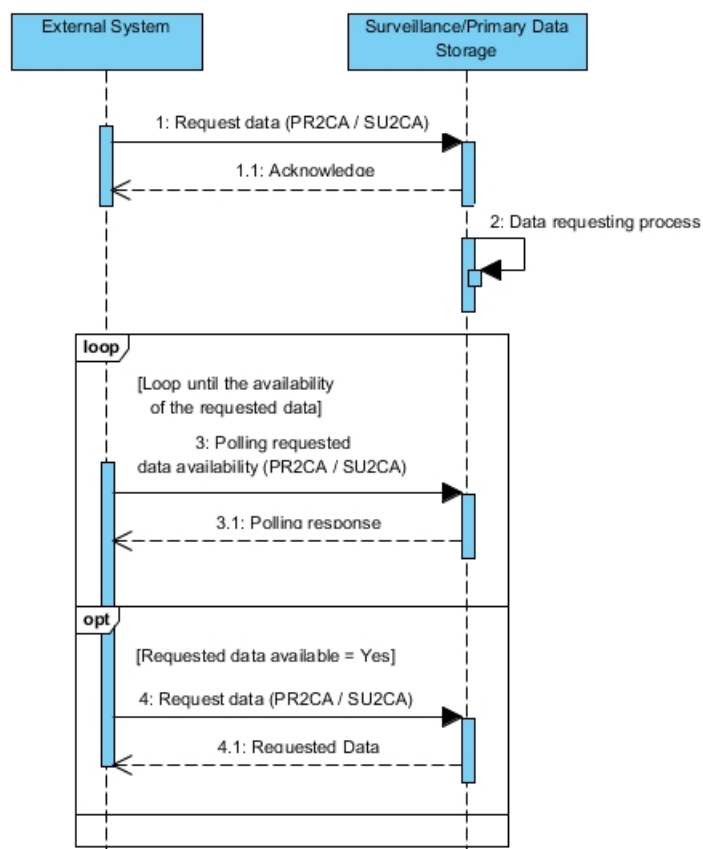
The diagram below depicts the sequence for external systems synchronously requesting data.



Sequence Description	
ID	Description
▪ 1	▪ External system synchronously requests data from the Surveillance Data Storage or to a Primary Data Storage using the respective correspondent SU2CA or PR2CA interfaces
▪ 1.1	▪ Requested Data Storage processes the data request
▪ 1.2	▪ Requested Data Storage sends the requested data back to the external system

3.2.3.2. Asynchronous request

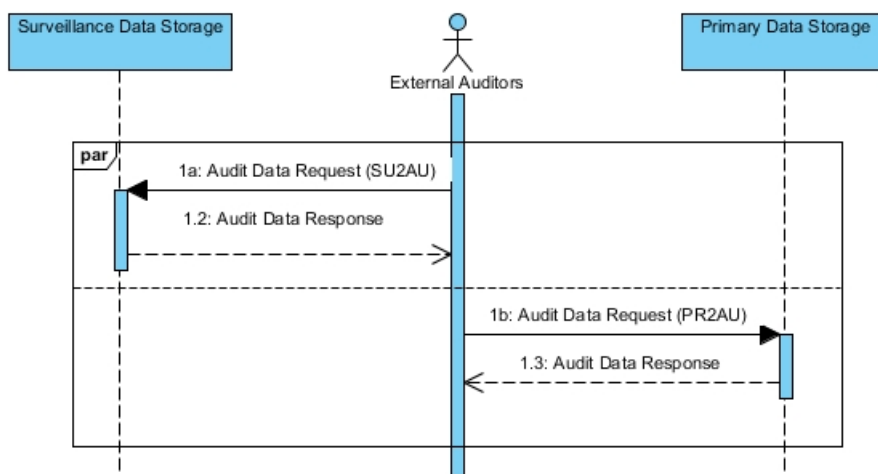
The diagram below depicts the sequence for an external system asynchronously requesting data.



Sequence Description	
ID	Description
▪ 1	▪ External system asynchronously requests data from the Surveillance Data Storage or to a Primary Data Storage using the respective correspondent SU2CA or PR2CA interfaces
▪ 1.1	▪ Requested Data Storage acknowledges the data request
▪ 2	▪ Requested Data Storage processes the data request
▪ 3	▪ External system checks the requested data availability using the respective correspondent SU2CA or PR2CA interfaces
▪ 3.1	▪ Requested Data Storage responses the requested data availability
▪ 4	▪ External system requests to retrieve the available data using the respective correspondent SU2CA or PR2CA interfaces
▪ 4.1	▪ Requested Data Storage responses the external system with the available data

3.2.4. Data auditing

The following diagram depicts the sequence for data auditing.



Sequence Description	
ID	Description
▪ 1a	▪ External auditor requests data from the Surveillance Data Storage using the SU2AU interface
▪ 1b	▪ External auditor requests data from the Primary Data Storage using the PR2AU interface
▪ 1.2	▪ Surveillance Data Storage sends the requested data to the external auditor
▪ 1.3	▪ Primary Data Storage sends the requested data to the external auditor

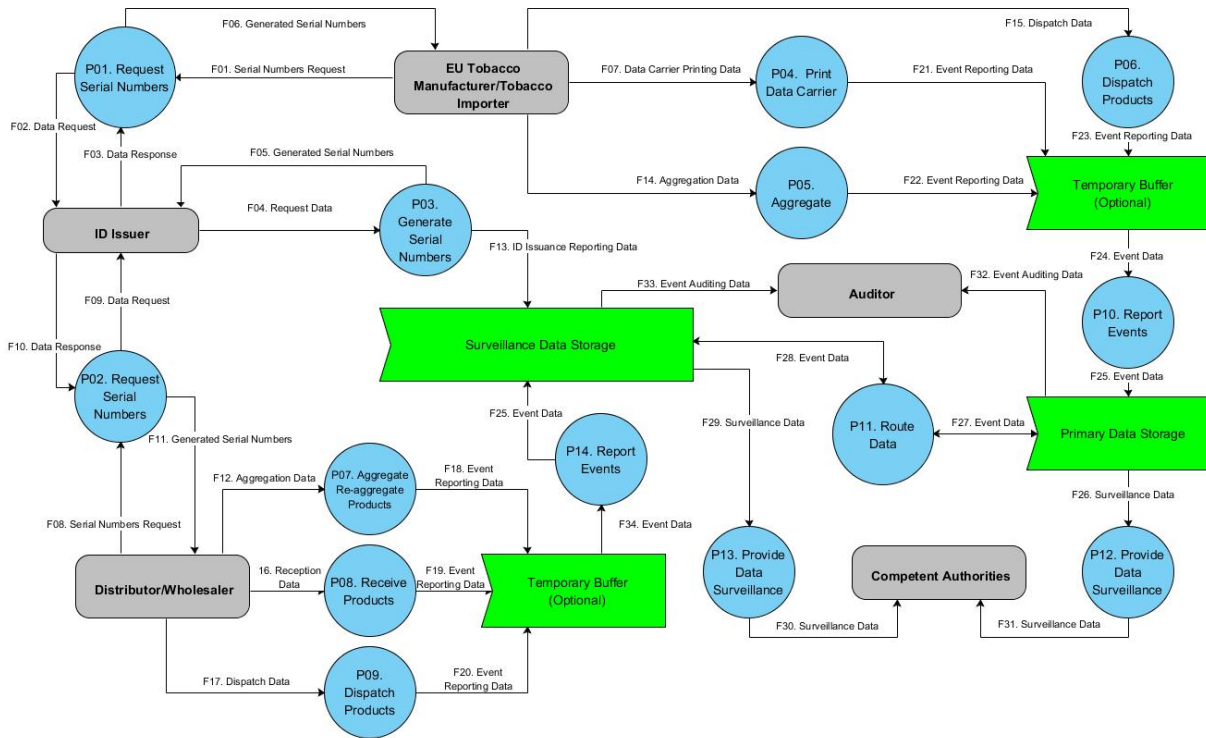
3.3. Data flow diagram

The diagram below depicts the data flow interaction between the external entities, the processes and the data repositories, with a high level view of the system.

Each data flow is further defined in the business process diagrams.

The interaction sequences are depicted in the sequence diagram. The interfaces are depicted in the System architecture diagram section.

Data Flow Diagram Description	
Symbol	Description
	A process or task that is performed by the system that activates the data flow.
	A Data Storage between processes.
	An initial source of data or any final destination for processed data.
	The direction of the data flow between a source and a destination.



3.4. Temporary Buffer (optional component)

3.4.1. Recommendation on the requirements to be accomplished

3.4.1.1. Functional

Recommended Functional Requirements – Tracking and Tracing System – Temporary Buffer		
ID	Name	Priority
RQ_TTTB_FU_1	Assurance of transmission of all relevant transactions	Must have
The Temporary Buffer shall ensure that all relevant transactions read by the economic operators are transmitted to either to a Primary Data Storage or to a Surveillance Data Storage facility.		
Source: Article 15(6) and 15(7) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTTB_FU_2	Raw Data Acquisition	Must have
The Temporary Buffer shall provide one interface through which a client (e.g. devices or systems from the facilities of the economic operators) may deliver one or more messages in raw format at a time.		
Source: Contractor’s expertise		
RQ_TTTB_FU_3	Data Format Transformation	Must have
The Temporary Buffer shall convert from the raw format used by the data provider to the one supported by the Tracking and Tracing System.		
Source: Contractor’s expertise		

Recommended Functional Requirements – Tracking and Tracing System – Temporary Buffer		
ID	Name	Priority
RQ_TTTB_FU_4	Data Format Validation	Must have
The Temporary Buffer shall validate the format of the message before sending it. Messages that are not conformant shall not be transmitted to the upper layer (i.e. Primary Data Storage and Surveillance Data Storage).		
Source: Contractor's expertise		
RQ_TTTB_FU_5	Transmission of Messages	Must have
The Temporary Buffer shall transmit the valid messages to the upper layer (i.e. Primary Data Storage and Surveillance Data Storage) through the interfaces described in sections 0 and 3.8.1.2.5.		
Source: Contractor's expertise		
RQ_TTTB_FU_6	Allowed delay for reporting	Must have
The Temporary Buffer shall send the valid messages to the upper layer (i.e. Primary Data Storage and Surveillance Data Storage) within the transmission time frame prescribed by the Implementing Regulation.		
Source: (everis, 2017)		
RQ_TTTB_FU_7	Logging of delivered messages	Should have
After the successful transmission of a message, the Temporary Buffer should register the transmission as accomplished in the log.		
Source: Contractor's expertise		
RQ_TTTB_FU_8	Management of delivered messages	Should have
After the successful transmission of a message, the Temporary Buffer should delete it from the local storage in order to save resources.		
Source: Contractor's expertise		

3.4.1.2. Technical

3.4.1.2.1. System qualities

System Qualities – Tracking and Tracing System – Temporary Buffer		
ID	Name	Priority
RQ_TTTB_RE_1	Message Replay-ability	Must have
The Temporary Buffer shall persist the outgoing messages until the messages are successfully delivered. When trying to transmit the outgoing messages, the Temporary Buffer shall handle transient failures by transparently retrying a failed operation.		
Source: Article 15(7) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTTB_RE_2	Data Reception Acknowledgment	Must have

System Qualities – Tracking and Tracing System – Temporary Buffer		
ID	Name	Priority
The Temporary Buffer shall send and acknowledgment to the sender (e.g. devices or systems from the facilities of the economic operators) regarding successful data receipt, otherwise failing with a consistent error code.		
Source: Contractor's expertise		
RQ_TTTB_RE_3	High Availability	Must have
The Temporary Buffer shall be available for use with an uptime target of 99.9%.		
Source: Contractor's expertise		
RQ_TTTB_RE_4	Outbound Channel Redundancy	Should have
The Temporary Buffer should be able to change automatically to additional outbound communication channels in case the message submission fails due to a communication error.		
Source: Contractor's expertise		
RQ_TTTB_PE_1	Minimum Processing Capacity	Must have
The Temporary Buffer shall be capable of processing one thousand (1,000) messages per minute as a minimum. The Temporary Buffer of each facility may have greater processing capacity in order to smoothly support the peak load estimated for that facility.		
Source: Contractor's expertise		
RQ_TTTB_PE_2	Minimum Concurrency Level	Must have
The Temporary Buffer shall support ten simultaneously connected clients. The Temporary Buffer of each facility may have a greater concurrency level in order to smoothly support the number of clients estimated for that facility.		
Source: Contractor's expertise		
RQ_TTTB_PE_3	Minimum Scalability	Must have
The Temporary Buffer shall support traffic spikes up to an average of 20% higher than normal demand.		
Source: Contractor's expertise		

3.4.1.2.2. Security

Security – Tracking and Tracing System – Temporary Buffer		
ID	Name	Priority
RQ_TTTB_SE_1	Sender Tracking	Must have
The Temporary Buffer shall resolve and authenticate the sender's identity against a trusted identity provider. Messages sent from an unauthenticated sender shall not be accepted.		

Security – Tracking and Tracing System – Temporary Buffer		
ID	Name	Priority
Source: Contractor’s expertise		
RQ_TTTB_SE_2	Checksum Verification	Must have
The Temporary Buffer shall verify the message checksum to ensure that the data was not tampered with. Messages where the checksum is not valid shall not be accepted.		
Source: Contractor’s expertise		

3.4.1.2.3. System constraints

System Constraints – Tracking and Tracing System – Temporary Buffer		
ID	Name	Priority
RQ_TTTB_SC_1	Data separation	Must have
The Temporary Buffer must separate data related to Tracking and Tracing System from other data of the economic operator company.		
Source: Recital 31 of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTTB_SC_2	Decoupling	Must have
The Temporary Buffer shall decouple data reception from data transmission, avoiding unnecessary coupling between processing of the data collected and the delivery of messages to the upper layer (i.e. Primary Data Storage and Surveillance Data Storage).		
Source: Contractor’s expertise		

3.5. Message

3.5.1. Requirements specification

3.5.1.1. Technical

3.5.1.1.1. System qualities

Technical Requirements – Tracking and Tracing System – Messaging		
ID	Name	Priority
RQ_TTME_RE_1	Retry Policy	Must have
The message exchange solution shall provide a retry policy.		
Source: Contractor’s expertise		
RQ_TTME_RE_2	Long-running process	Must have

Technical Requirements – Tracking and Tracing System – Messaging		
ID	Name	Priority
The message exchange solution shall reply to parties' messages that invoke a long-running process with an identification of the request for future retrieval of the results.		
Source: Contractor's expertise		
RQ_TTME_RE_3	Error handling	Should have
The message exchange solution should provide an error handling mechanism.		
Source: Contractor's expertise		
RQ_TTME_RE_4	Error handling – throw exception	Should have
The error handling mechanism should manage fails and throw an exception, allowing error management.		

3.5.1.1.2. Security

Technical Requirements – Tracking and Tracing System – Messaging		
ID	Name	Priority
RQ_TTME_SE_1	Message Exchange - Users Authentication	Must have
Users shall be authenticated to exchange messages, using an authentication mechanisms such as TLS/SSL.		
Source: Contractor's expertise		
RQ_TTME_SE_2	Message Exchange - Communication Channel Security	Must have
The exchange of messages shall be performed through a secure communication channel using a cryptographic protocol such as TLS/SSL.		
Source: Contractor's expertise		
RQ_TTME_SE_3	Message Exchange – Data hacking	Must have
The exchange of messages shall comprise security verification and code best practices, including data sanitization and data validation in order to prevent the risk of data hacking and vulnerabilities, such as SQL injection techniques.		
Source: Contractor's expertise		

3.5.1.1.3. System constraints

Technical Requirements – Tracking and Tracing System – Messaging		
ID	Name	Priority
RQ_TTME_SC_1	Extensibility	Must have
The message specification shall include some extensibility mechanism in order to support the exchange of additional fields or event types, if necessary.		
Source: Contractor's expertise		

Technical Requirements – Tracking and Tracing System – Messaging		
ID	Name	Priority
RQ_TTME_SC_2	Extensibility – New Message Type	Must have
The message specification shall include some extensibility mechanism in order to support that new event types could be added.		
Source: Contractor's expertise		
RQ_TTME_SC_3	Extensibility – New Field	Must have
The message specification shall include some extensibility mechanism in order to support that new fields could be added to an existing event type.		
The message shall be extensible, allowing new fields to be added to an existing message type. The bindings, capture interface, and query interfaces shall be designed to permit this type of extension without requiring changes to the specification itself.		
Source: Contractor's expertise		
RQ_TTME_SC_4	Message Exchange - Schema	Must have
The message exchange system shall provide the communication parties a way to obtain the available structure schemas of messages, including the version of the schema.		
Source: Contractor's expertise		
RQ_TTME_SC_5	Message Exchange – Call service	Must have
The message exchange system shall provide synchronous and asynchronous call services.		
Source: Contractor's expertise		
RQ_TTME_SC_6	Splitting a Message	Must have
The message exchange shall support a message splitting mechanism in order to avoid surpassing the maximum allowed message size.		
Source: Contractor's expertise		
RQ_TTME_SC_7	Collection of Events	Must have
The message specification shall support the sending of a collection of events.		
Source: Contractor's expertise		
RQ_TTME_SC_8	Message Traceability	Must have
The message exchange solution shall provide the message traceability.		
Source: Contractor's expertise		
RQ_TTME_SC_9	Message Structure	Must have
The message format structure shall be conformant with the section 3.5.2 format specification.		
Source: Contractor's expertise		

3.5.1.2. Applicable standards

Technical Requirements – Tracking and Tracing System – Messaging		
ID	Name	Priority
RQ_TTME_AS_1	Message Exchange System	Must have
The message exchange system shall be performed through a web service solution using HTTP/HTTPS as communication protocol.		
Source: Contractor's expertise		
RQ_TTME_AS_2	Message Coding Format	Must have
Messages shall be formed with the XML (W3C XML, 2016) standard format. As a future enhancement, the System should also be able to support other widely-adopted coding formats such as JSON.		
Source: Contractor's expertise		
RQ_TTME_AS_3	Character set encoding	Must have
Messages shall be encoded using the ISO/IEC 8859-15:1999 character set.		
Source: Contractor's expertise		
RQ_TTME_AS_4	ISO/IEC 19987:2015 EPCIS compatibility	Must have
The messages structure shall be compatible with the (ISO/IEC 19987:2015 EPCIS, 2016) standard, when possible, to the data storages.		
Source: Contractor's expertise		

3.5.2. Format specification

The table below shows the different message types to be supported by the System, including the interfaces that manage them:

Process	Message Type	Description	Interfaces
Registration	REO	Message to request the registration of an economic operator	II2EO
	CEO	Message to request the information correction of an economic operator	
	DEO	Message to request the de-registration of an economic operator	
	RFA	Message to request the registration of a tobacco facility	
	CFA	Message to request the information correction of a tobacco facility	
	DFA	Message to request the de-registration of a tobacco facility	
	RMA	Message to request the registration of a tobacco machine	
	CMA	Message to request the information correction of a tobacco machine	
	DMA	Message to request the de-registration of a tobacco machine	

Process	Message Type	Description	Interfaces
Issuance of serial numbers	ISU	Message to request the issuance of serial numbers at unit packet level	II2EO
	RSU	Message to retrieve the issued serial numbers at unit packet level	
	ISA	Message to request the issuance of serial numbers at aggregated level	
	RSA	Message to retrieve the issued serial numbers at aggregated level	
	IDA	Message to request a UID deactivation	PR2MI PR2SU SU2DW SU2PR SU2II
	IRU	Message to report the issuance of serial numbers at unit packet level	SU2II
	IRA	Message to report the issuance of serial numbers at aggregated level	
Operational	EUA	Message to report an UID application event	PR2MI PR2SU SU2DW SU2PR SU2II
	EPA	Message to report an aggregation event	
	EDP	Message to report a dispatch event	
	ERP	Message to report a reception event	
	ETL	Message to report a trans-loading event	
	EUD	Message to report an UID disaggregation	
	EVR	Message to report the delivery carried out with a vending van to retail outlet	
Transactional	EIV	Message to report an invoice	PR2MI PR2SU SU2DW SU2PR SU2II
	EPR	Message to report a payment record	
	EPO	Message to report a purchase order	
Recall	RCL	Message to recall another message	II2EO PR2MI SU2DW
Data extraction from the data storages	DRX	Message to request data extraction from the Data Storages	PR2CA PR2AU SU2CA SU2AU
	DTX	Message to retrieve extracted data from the Data Storages	

Table 38: Types of messages to be exchanged through the Tracking and Tracing System

The message specification follows the approach below:

- The schema of each **request message** comprises the following blocks of information elements:
 - A **common** block, which refers to information shared by all the requests (i.e. message type, message time, sender identifier, and an extensibility component). The extensibility component aims at establishing a mechanism to include additional fields in the future, if necessary.

- A **specific** block, which includes particular elements of information related to the specific message type.
- Likewise, the schema of each **response message** comprises the following blocks of elements:
 - A **common** block, which refers to information shared by all the responses (i.e. message type, message time, sender identifier, error component, a code of acknowledgment, and an extensibility component). The extensibility component aims at establishing a mechanism to include additional fields in the future if necessary.
 - A **specific** block, which includes particular elements of information related to the specific message type.
- The common blocks are described at the beginning of this chapter. The specific blocks of elements are described for each message type in separate sections.
- For each message type, the schema structure of the request is specified, as well as the response.

Finally, a **mapping to the ISO/IEC 19987:2015 EPCIS Data Definition and Service layers is provided** for the following message types:

- Operational events:
 - UID application
 - Aggregation
 - Dispatch
 - Reception
 - Trans-loading
- Transactional events:
 - Invoice
 - Purchase
 - Payment

In this respect, it should be noted that ISO/IEC 19987:2015 EPCIS is devoted to managing supply chain visibility events. Hence, some of the data requirements of the System (i.e. registration, issuance of serial numbers, data extraction from the repositories, and message recall) cannot be mapped to the ISO/IEC 19987:2015 EPCIS schemas.

3.5.2.1. Common schema elements

3.5.2.1.1. Basic information block concerning the request

Basic information block concerning the request - schema					
Field	Description	Data Type	Cardinality	Priority	Values
M_Type	The identifier of the type of message	Text	S	M	See above types of messages list
M_Time	The timestamp up to the second in UTC when this message has been created	Timestamp(L)	S	M	
Sender_ID	The identifier of the economic operator sending the message	EOID	S	M	

Basic information block concerning the request - schema					
Field	Description	Data Type	Cardinality	Priority	Values
Extensibility element	This field shall contain the schema extension element structure according to any new data holder type needed in the future	Component <<schema extension element>>	S	O	

3.5.2.1.2. Basic information block concerning the response

Basic information block concerning the response - schema					
Field	Description	Data Type	Cardinality	Priority	Values
M_Type	The identifier of the type of message that the response refers to	Text	S	M	See above types of messages list
M_Time	The date and time in UTC when this message has been created	Timestamp(L)	S	M	
Sender_ID	The identifier of the ID Issuer which responds to the message	TSID	S	M	
Error	Indicates the failure of the message reception	Boolean	S	M	0 – No 1- Yes
Error_Code	The code which indicates the error related to the failure of the reception	Text	S	M if Error = 1	System error catalogue
Error_Descr	The description of the error related to the failure of the reception. The error description should be specific enough to find answers, solutions and detect potential errors at the level of individual UIs if possible. (E.g. in the message for aggregation of a master case, there is one erroneous UI at the level of cartons (which means that other 49 carton UIs and the aggregated UI are correct), the error message should point at this one erroneous UI.)	Text	S	M if Error = 1	
CODE	The internal code of acknowledgment of the message	Text	S	M if Error = 0	
Extensibility element	This field shall contain the schema extension element structure according to any new data holder type needed in the future	Component <<schema extension element>>	S	O	

3.5.2.2. Registration messages

3.5.2.2.1. Registration of economic operator

Request:

registration of economic operator – request					
Field	Description	Data Type	Cardinality	Priority	Values

registration of economic operator – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = REO
EO_Name1	Economic operator's registered name	Text	S	M	
EO_Name2	Economic operator's alternative or abridged name	Text	S	O	
EO_Address	Economic operator's address – street name, house number, postal code, city	Text	S	M	
EO_CountryReg	Economic operator's country of registration	Country	S	M	See Country in section 3.11.4.6
EO_Email	Economic operator's email address; used to inform about registration process, incl. subsequent changes and other required correspondence	Text	S	M	
VAT_R	Indication of the VAT registration status	Boolean	S	M	0 – No VAT registration 1 – VAT number exists
VAT_N	Economic operator's VAT number	Text	S	M, if VAT_R = 1	
TAX_N	Economic operator's tax registration number	Text	S	M, if VAT_R = 0	
EO_ExciseNumber1	Indication if the economic operator has an excise number issued by the competent authority for the purpose of identification of persons/premises	Boolean	S	M	0 – No SEED number 1 – SEED number exists
EO_ExciseNumber2	Economic operator's excise number issued by the competent authority for the purpose of identification of persons/premises	SEED	S	M, if EO_ExciseNumber1 = 1	
OtherEOID_R	Indication if the economic operator has been allocated an identifier by another ID Issuer	Boolean	S	M	0 – No 1 – Yes
OtherEOID_N	Economic operator identifier codes allocated by other ID Issuers	EOID	M	M, if OtherEOID_R = 1	
Reg_3RD	Indication if the registration is made on behalf of a retail outlet operator not otherwise involved in the tobacco trade	Boolean	S	M	0 – No 1 – Yes
Reg_EOID	Identifier of the economic operator that acts on behalf of a retail outlet operator not otherwise involved in the tobacco trade	EOID	S	M, if Reg_3RD = 1	

Response:

registration of economic operator – response
--

Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = REO
EO_ID	Economic operator's identifier registered	EOID	S	M if Error = 0	

3.5.2.2.2. Correction of information concerning the economic operator

Request:

correction of information concerning the economic operator – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = CEO
EO_ID	Economic operator identifier code	EOID	S	M	
EO_CODE	Economic operator's confirmation code provided in response to the registration of economic operator	Text	S	M	
EO_Name1	Economic operator's registered name	Text	S	M	
EO_Name2	Economic operator's alternative or abridged name	Text	S	O	
EO_Address	Economic operator's address – street name, postal code and city	Text	S	M	
EO_CountryReg	Economic operator's country of registration	Country	S	M	See Country in section 3.11.4.6
EO_Email	Economic operator's email address – used to inform about registration process, incl. subsequent changes	Text	S	M	
VAT_R	Indication of the VAT registration status	Boolean	S	M	0 – No VAT registration 1 – VAT number exists
VAT_N	Economic operator's VAT number	Text	S	M, if VAT_R = 1	
TAX_N	Economic operator's tax registration number	Text	S	M, if VAT_R = 0	
EO_ExciseNumber1	Indication if the economic operator has an excise number issued by the competent authority for the purpose of identification of persons/premises	Boolean	S	M	0 – No SEED number 1 – SEED number exists
EO_ExciseNumber2	Economic operator's excise number issued by the competent authority for the purpose of identification of persons/premises	SEED	S	M, if EO_ExciseNumber1 = 1	
OtherEOID_R	Indication if the economic operator has been allocated an identifier by another ID	Boolean	S	M	0 – No

correction of information concerning the economic operator – request					
Field	Description	Data Type	Cardinality	Priority	Values
	Issuer				1 – Yes
OtherEOID_N	Economic operator identifier codes allocated by other ID Issuers	EOID	M	M, if OtherEOID_R = 1	
Reg_3RD	Indication if the registration is made on behalf of a retail outlet operator not otherwise involved in the tobacco trade	Boolean	S	M	0 – No 1 – Yes
Reg_EOID	Identifier of the economic operator that acts on behalf of a retail outlet operator not otherwise involved in the tobacco trade	EOID	S	M, if Reg_3RD = 1	

Response:

correction of information concerning the economic operator – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = CEO

3.5.2.2.3. De-registration of economic operator

Request:

de-registration of economic operator – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = DEO
EO_ID	Economic operator identifier code	EOID	S	M	
EO_CODE	Economic operator's confirmation code provided in response to the registration of economic operator	Text	S	M	
Reg_3RD	Indication if the registration is made on behalf of a retail outlet operator not otherwise involved in the tobacco trade	Boolean	S	M	0 – No 1 – Yes
Reg_EOID	Identifier of the economic operator that acts on behalf of a retail outlet operator not otherwise involved in the tobacco trade	EOID	S	M, if Reg_3RD = 1	

Response:

De-registration of economic operator – response					
---	--	--	--	--	--

Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = DEO

3.5.2.2.4. Registration of facility

Request:

registration of facility – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = RFA
EO_ID	Economic operator identifier code	EOID	S	M	
EO_CODE	Economic operator's confirmation code provided in response to the registration of economic operator	Text	S	M	
F_Address	Facility's address – street name, house number, postal code and city	Text	S	M	
F_Country	Facility's country	Country	S	M	See Country in section 3.11.4.6
F_Type	Type of facility	Integer	S	M	See FacilityType in section 3.11.4.6
F_Type_Other	Description of other facility type	Text	S	M, if F_Type = 4	
F_Status	Indication if a part of the facility has a bonded warehouse status	Boolean	S	M	0 – No 1 – Yes
F_ExciseNumber1	Indication if the facility has an excise number issued by the competent authority for the purpose of identification of persons/premises	Boolean	S	M	0 – No SEED number 1 – SEED number exists
F_ExciseNumber2	Facility's excise number issued by the competent authority for the purpose of identification of persons/premises	SEED	S	M, if F_ExciseNumber1 = 1	
OtherFID_R	Indication if the facility has been allocated an identifier by another ID Issuer	Boolean	S	M	0 – No 1 – Yes (possible only for non-EU facilities)
OtherFID_N	Facility identifier codes allocated by other ID Issuers	FID	M	M, if OtherFID_R = 1	
Reg_3RD	Indication if the registration is made on behalf of a retail outlet operator not otherwise involved in the tobacco trade	Boolean	S	M	0 – No 1 – Yes (possible only if F_Type = 3)

registration of facility – request					
Field	Description	Data Type	Cardinality	Priority	Values
Reg_EOID	Identifier of the economic operator that acts on behalf of a retail outlet operator not otherwise involved in the tobacco trade	EOID	S	M, if Reg_3RD = 1	

Response:

registration of facility – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = RFA
F_ID	Facility's identifier registered	FID	S	M if Error = 0	

3.5.2.2.5. Correction of information concerning the facility

Request:

correction of information concerning the facility – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = CFA
EO_ID	Economic operator identifier code	EOID	S	M	
EO_CODE	Economic operator's confirmation code provided in response to the registration of economic operator	Text	S	M	
F_ID	Facility identifier code	FID	S	M	
F_Address	Facility's address – street name, postal code and city	Text	S	M	
F_Country	Facility's country	Country	S	M	See Country in section 3.11.4.6
F_Type	Type of facility	Integer	S	M	See FacilityType in section 3.11.4.6
F_Type_Other	Description of other facility type	Text	S	M, if F_Type = 4	
F_Status	Indication if a part of the facility has a bonded warehouse status	Boolean	S	M	0 – No 1 – Yes
F_ExciseNumber1	Indication if the facility has an excise number issued by the competent authority for the purpose of identification of persons/premises	Boolean	S	M	0 – No SEED number 1 – SEED number exists

correction of information concerning the facility – request					
Field	Description	Data Type	Cardinality	Priority	Values
F_ExciseNumber2	Facility's excise number issued by the competent authority for the purpose of identification of persons/premises	SEED	S	M, if F_ExciseNumber1 = 1	
OtherFID_R	Indication if the facility has been allocated an identifier by another ID Issuer	Boolean	S	M	0 – No 1 – Yes (possible only for non-EU facilities)
OtherFID_N	Facility identifier codes allocated by other ID Issuers	FID	M	M, if OtherFID_R = 1	
Reg_3RD	Indication if the registration is made on behalf of a retail outlet operator not otherwise involved in the tobacco trade	Boolean	S	M	0 – No 1 – Yes (possible only if F_Type = 3)
Reg_EOID	Identifier of the economic operator that acts on behalf of a retail outlet operator not otherwise involved in the tobacco trade	EOID	S	M, if Reg_3RD = 1	

Response:

correction of information concerning the facility – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = CFA

3.5.2.2.6. De-registration of facility

Request:

de-registration of facility – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = DFA
EO_ID	Economic operator identifier code	EOID	S	M	
EO_CODE	Economic operator's confirmation code provided in response to the registration of economic operator	Text	S	M	
F_ID	Facility identifier code	FID	S	M	
Reg_3RD	Indication if the de-registration is made on behalf of a retail outlet operator not	Boolean	S	M	0 – No

de-registration of facility – request					
Field	Description	Data Type	Cardinality	Priority	Values
	otherwise involved in the tobacco trade				1 – Yes
Reg_EOID	Identifier of the economic operator that acts on behalf of a retail outlet operator not otherwise involved in the tobacco trade	EOID	S	M, if Reg_3RD = 1	

Response:

de-registration of facility – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = DFA

3.5.2.2.7. Registration of manufacturing machine

Request:

registration of manufacturing machine – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = RMA
EO_ID	Economic operator identifier code	EOID	S	M	
EO_CODE	Economic operator's confirmation code provided in response to the registration of economic operator	Text	S	M	
F_ID	Facility identifier code	FID	S	M	
M_Producer	Machine producer	Text	S	M	
M_Model	Machine model	Text	S	M	
M_Number	Machine serial number	Text	S	M	
M_Capacity	Maximum capacity over 24-hour production cycle expressed in unit packets	Integer	S	M	

Response:

registration of manufacturing machine – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = RMA
M_ID	Manufacturing machine identifier registered	MID	S	M if Error = 0	

3.5.2.2.8. Correction of information concerning the manufacturing machine

Request:

correction of information concerning the manufacturing machine – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = CMA
EO_ID	Economic operator identifier code	EOID	S	M	
EO_CODE	Economic operator's confirmation code provided in response to the registration of economic operator	Text	S	M	
F_ID	Facility identifier code	FID	S	M	
M_ID	Machine identifier code	MID	S	M	
M_Producer	Machine producer	Text	S	M	
M_Model	Machine model	Text	S	M	
M_Number	Machine serial number	Text	S	M	
M_Capacity	Maximum capacity over 24-hour production cycle expressed in unit packets	Integer	S	M	

Response:

correction of information concerning the manufacturing machine – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = CMA

3.5.2.2.9. De-registration of manufacturing machine

Request:

de-registration of manufacturing machine – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = DMA
EO_ID	Economic operator identifier code	EOID	S	M	
EO_CODE	Economic operator's confirmation code provided in response to the registration of economic operator	Text	S	M	
F_ID	Facility identifier code	FID	S	M	
M_ID	Machine identifier code	MID	S	M	

Response:

De-registration of manufacturing machine – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = DMA

3.5.2.3. Issuance of serial numbers messages

3.5.2.3.1. Request for the issuance of serial numbers at unit packet level

Request:

request for the issuance of serial numbers at unit packet level – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = ISU
EO_ID	Economic operator identifier code of the submitting entity (either EU manufacturer or EU importer)	E OID	S	M	
F_ID	Facility identifier code	F ID	S	M	
Process_Type	Indication if the production process involves machinery	Boolean	S	M	0 – No (only for fully hand made products) 1 – Yes
M_ID	Machine identifier code	M ID	S	M	
P_Type	Type of tobacco product	Integer	S	M	See TobaccoProductType in section 3.11.4.6
P_OtherType	Description of other type of tobacco product	Text	S	M, if P_Type = 12 (other tobacco product)	
P_Brand	Brand of tobacco product	Text	S	M	
P_weight	Average gross weight of unit packet, including packaging, in grams with 0.1 gram accuracy	Decimal	S	M	
TP_ID	The identification number of the product used in the EU-CEG system	TP ID	S	M, if Intended_Market is an EU country	
TP_PN	Tobacco product number used in the EU-CEG system	PN	S	M, if Intended_Market is an EU country	
Intended_Market	Intended country of retail sale	Country	S	M	

request for the issuance of serial numbers at unit packet level – request					
Field	Description	Data Type	Cardinality	Priority	Values
Intended_Route1	Indication if the product is intended to be moved across country borders with terrestrial transport	Boolean	S	M	0 – No 1 – Yes
Intended_Route2	The first country of terrestrial transport after the product leaves the Member State of manufacturing or the Member State of importation	Country	S	M, if Intended_Route1 = 1	
Import	Indication if the product is imported into the EU	Boolean	S	M	0 – No 1 – Yes
Req_Quantity	Requested quantity of unit packet level UIs	Integer	S	M	

Response:

request for the issuance of serial numbers at unit packet level – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = ISU

3.5.2.3.2. Retrieve the issued serial numbers at unit packet level

Request:

retrieve the issued serial numbers at unit packet level – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = RSU
EO_ID	Economic operator identifier code of the submitting entity (either EU manufacturer or EU importer)	EOID	S	M	
Issuance_Req_CODE	The previously given identifier of the serial numbers issuance request	Text	S	M	

Response:

retrieve the issued serial numbers at unit packet level – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = RSA

retrieve the issued serial numbers at unit packet level – response					
Field	Description	Data Type	Cardinality	Priority	Values
upUI	List of unit packet level UIs	upUI(s)	M	M, if Error = 0	

3.5.2.3.3. Request for reporting the issuance of serial numbers at unit packet level

Request:

request for reporting the issuance of serial numbers at unit packet level – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = IRU
EO_ID	Economic operator identifier code of the submitting entity (either EU manufacturer or EU importer)	E OID	S	M	
F_ID	Facility identifier code	FID	S	M	
Process_Type	Indication if the production process involves machinery	Boolean	S	M	0 – No (only for fully hand made products) 1 – Yes
M_ID	Machine identifier code	MID	S	M	
P_Type	Type of tobacco product	Integer	S	M	See TobaccoProductType in section 3.11.4.6
P_OtherType	Description of other type of tobacco product	Text	S	M, if P_Type = 12 (other tobacco product)	
P_Brand	Brand of tobacco product	Text	S	M	
P_weight	Average gross weight of unit packet, including packaging, in grams with 0.1 gram accuracy	Decimal	S	M	
TP_ID	The identification number of the product used in the EU-CEG system	TPID	S	M, if Intended_Market is an EU country	
TP_PN	Tobacco product number used in the EU-CEG system	PN	S	M, if Intended_Market is an EU country	
Intended_Market	Intended country of retail sale	Country	S	M	
Intended_Route1	Indication if the product is intended to be moved across country borders with terrestrial transport	Boolean	S	M	0 – No 1 – Yes
Intended_Route2	The first country of terrestrial transport after the product	Country	S	M, if Intended	

request for reporting the issuance of serial numbers at unit packet level – request					
Field	Description	Data Type	Cardinality	Priority	Values
	leaves the Member State of manufacturing or the Member State of importation			_Route1 = 1	
Import	Indication if the product is imported into the EU	Boolean	S	M	0 – No 1 – Yes
Req_Quantity	Requested quantity of unit packet level UIs	Integer	S	M	
upUI	List of unit packet level UIs issued	upUI(s)	M	M	

Response:

request for reporting the issuance of serial numbers at unit packet level – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = IRU

3.5.2.3.4. Request for the issuance of serial numbers at aggregated level

Request:

request for the issuance of serial numbers at aggregated level – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = ISA
EO_ID	Economic operator identifier code of the submitting entity	EOID	S	M	
F_ID	Facility identifier code	FID	S	M	
Req_Quantity	Requested quantity of aggregated level UIs	Integer	S	M	

Response:

request for the issuance of serial numbers at unit packet level – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = ISA

3.5.2.3.5. Retrieve the issued serial numbers at aggregated level

Request:

retrieve the issued serial numbers at aggregated level – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = RSA
EO_ID	Economic operator identifier code of the submitting entity (either EU manufacturer or EU importer)	EOID	S	M	
Issuance_Req_CODE	The previously given identifier of the serial numbers issuance request	Text	S	M	

Response:

retrieve the issued serial numbers at aggregated level – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = RSA
aUI	List of aggregated level UIs	aUI	M	M, if Error = 0	

3.5.2.3.6. Request for reporting the issuance of serial numbers at aggregated level

Request:

request for reporting the issuance of serial numbers at aggregated level – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = IRA
EO_ID	Economic operator identifier code of the submitting entity	EOID	S	M	
F_ID	Facility identifier code	FID	S	M	
Req_Quantity	Requested quantity of aggregated level UIs	Integer	S	M	
aUI	List of aggregated level UIs	aUI	M	M	

Response:

request for reporting the issuance of serial numbers at aggregated level – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = IRA

3.5.2.3.7. Request for deactivation of UIs

Request:

request for the deactivation of UIs – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = IDA
EO_ID	Economic operator identifier code of the submitting entity	EOID	S	M	
Deact_Type	Deactivation of unit packet or aggregated level UIs	Integer	S	M	1 – Unit pack level UIs 2 – Aggregated level UIs
Deact_Reason_1	Identification of the reason for deactivation	Integer	S	M	See DeactivationReasonType in section 3.11.4.6
Deact_Reason_2	Description of other reason	Text	S	M, if Deact_Reason1 = 6 (other reason)	
Deact_Reason_3	Additional description of the reason	Text	S	O	
Deact_upUI	List of unit packet level UIs to be deactivated	upUI(s)	M	M, if Deact_Type = 1	
Deact_aUI	List of aggregated level UIs to be deactivated	aUI	M	M, if Deact_Type = 2	

Response:

request for the deactivation of UIs – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = IDA

3.5.2.4. Operational event messages

3.5.2.4.1. Application of unit level UIs on unit packets event

Request:

UID application event					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = EUA

UID application event					
Field	Description	Data Type	Cardinality	Priority	Values
EO_ID	Economic operator identifier code of the submitting entity	EOID	S	M	
F_ID	Facility identifier code	FID	S	M	
Event_Time	Time of event occurrence	Time(s)	S	M	
upUI_1	List of unit packet level UIs to be recorded (full length)	upUI(L)	M	M	
upUI_2	List of corresponding unit packet level UIs to be recorded (as visible in human readable format) indicated in the same order as upUI_1	upUI(s)	M	M	
upUI_comment	Comments by the reporting entity	Text	S	O	

Response:

UID application event – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = EUA

3.5.2.4.2. Application of aggregated level UIs on aggregated packaging event

Request:

Aggregation event					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = EPA
EO_ID	Economic operator identifier code of the submitting entity	EOID	S	M	
F_ID	Facility identifier code	FID	S	M	
Event_Time	Time of event occurrence	Time(s)	S	M	
aUI	Aggregated level UI	aUI	S	M	
Aggregation_Type	Identification of aggregation type	Integer	S	M	1 – aggregation of only unit packet level UIs 2 – aggregation of only aggregated level UIs 3 – aggregation of both unit packet and aggregated level UIs
Aggregated_UIs1	List of unit packet level UIs subject to aggregation	upUI(L)	M	M, if Aggregation_Type = 1 or 3	

Aggregation event					
Field	Description	Data Type	Cardinality	Priority	Values
Aggregated_UIs2	List of aggregated level UIs subject to further aggregation	aUI	M	M, if Aggregation_Type = 2 or 3	
upUI_comment	Comments by the reporting entity	Text	S	O	

Response:

Aggregation event – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = EPA

3.5.2.4.3. Dispatch of tobacco products from a facility (Dispatch) event

Request:

Dispatch event					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = EDP
EO_ID	Economic operator identifier code of the submitting entity	EOID	S	M	
Event_Time	Time of event occurrence	Time(s)	S	M	
F_ID	Dispatch facility identifier code	FID	S	M	
Destination_ID1	Indication of destination type: if the destination facility is located on the EU territory and if it is delivery to a vending machine (VM) or by means of a vending van (VV) delivering to multiple retail outlets in quantities that have not been predetermined in advance of the delivery	Integer	S	M	1 – Non EU dest. 2 – EU destination other than VM – fixed quantity delivery 3 – EU VM(s) 4 – EU destination other than VM – delivery with VV
Destination_ID2	Destination facility identifier code	FID	S	M, if Destination_ID1 = 2	
Destination_ID3	Destination facility identifier code(s) – possible multiple vending machines	FID	M	M, if Destination_ID1 = 3	
Destination_ID4	Destination facility identifier code(s)	FID	M	M, if Destination_ID1	

Dispatch event					
Field	Description	Data Type	Cardinality	Priority	Values
				= 4	
Destination_ID5	Destination facility's full address: street, house number, postal code, city	Text	S	M, if Destination_ID1 = 1	
Transport_mode	Mode of transport by which the product leaves the facility, see: Commission Regulation (EC) No 684/2009, Annex 2, Code List 7	Integer	S	M	0 - Other 1 - Sea Transport 2 - Rail transport 3 - Road transport 4 - Air transport 5 - Postal consignment 7 - Fixed transport installations 8 - Inland waterway transport
Transport_vehicle	Identification of the vehicle (i.e. number plates, train number, plane/flight number, ship name or other identification)	Text	S	M	'n/a' is permitted value if Transport_mode = 0 and product movement takes place between adjacent facilities and is delivered manually
Transport_container1	Indication if the transport is containerised and uses an individual transport unit code (e.g. SSCC)	Boolean	S	M	0 - No 1 - Yes
Transport_container2	Individual transport unit code of the container	ITU	S	M, if Transport_container1 = 1	
Transport_s1	Indication if the dispatch takes place with the logistic/postal operator who operates its own track and trace system accepted by the Member State of the dispatch facility. Only for small quantities of tobacco products (net weight of the products dispatched below 10kg) destined for exports to third countries.	Boolean	S	M	0 - No 1 - Yes
Transport_s2	The logistic operator's tracking number	Text	S	M, if Transport_s1 = 1	
EMCS	Dispatch under the Excise Movement and Control System (EMCS)	Boolean	S	M	0 - No

Dispatch event					
Field	Description	Data Type	Cardinality	Priority	Values
					1 – Yes
EMCS_ARC	Administrative Reference Code (ARC)	ARC	S	M, if EMCS = 1	
SAAD	Dispatch with a simplified accompanying document, see: Commission Regulation (EEC) No 3649/92	Boolean	S	M	0 – No 1 – Yes
SAAD_number	Reference number of the declaration and/or authorization which has to be given by the competent authority in the Member State of destination before the movement starts	Text	S	M, if SAAD = 1	
Exp_Declaration	Indication if the Movement Reference Number (MRN) has been issued by the customs office	Boolean	S	M	0 – No 1 – Yes
Exp_DeclarationNumber	Movement Reference Number (MRN)	MRN	S	M, if Exp_Declaration = 1	
UI_Type	Identification of UI types in the dispatch (recorded at the highest level of available aggregation)	Integer	S	M	1 – only unit packet level UIs 2 – only aggregated level UIs 3 – both unit packet and aggregated level UIs
upUIs	List of unit packet level UIs subject to the dispatch	upUI(L)	M	M, if UI_Type = 1 or 3	
aUIs	List of aggregated level UIs subject to the dispatch	aUI	M	M, if UI_Type = 2 or 3	
Dispatch_comment	Comments by the reporting entity	Text	S	0	

Response:

Dispatch event – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = EDP

3.5.2.4.4. Arrival of tobacco products at a facility (Reception) event

Request:

Reception event					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = ERP
EO_ID	Economic operator identifier code of the submitting entity	EOID	S	M	
F_ID	Arrival facility identifier code	FID	S	M	
Event_Time	Time of event occurrence	Time(s)	S	M	
Product_Return	Indication if the arriving products are a return following complete or partial non-delivery	Boolean	S	M	0 – No 1 – Yes
UI_Type	Identification of UI types received (recorded at the highest level of available aggregation)	Integer	S	M	1 – only unit packet level UIs 2 – only aggregated level UIs 3 – both unit packet and aggregated level UIs
upUIs	List of unit packet level UIs received	upUI(L)	M	M, if UI_Type = 1 or 3	
aUIs	List of aggregated level UIs received	aUI	M	M, if UI_Type = 2 or 3	
Arrival_comment	Comments by the reporting entity	Text	S	O	

Response:

Reception event – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = ERP

3.5.2.4.5. Trans-loading event

Request:

Trans-loading event					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = ETL
EO_ID	Economic operator identifier code of the submitting entity	EOID	S	M	

Trans-loading event					
Field	Description	Data Type	Cardinality	Priority	Values
Event_Time	Time of event occurrence	Time(s)	S	M	
Destination_ID1	Indication if the destination facility is located on the EU territory	Boolean	S	M	0 – No 1 – Yes
Destination_ID2	Destination facility identifier code	FID	S	M, if Destination_ID1 = 1	
Destination_ID3	Destination facility's full address	Text	S	M, if Destination_ID1 = 0	
Transport_mode	Mode of transport to which the product is trans-loaded, see: Commission Regulation (EC) No 684/2009, Annex 2, Code List 7	Integer	S	M	0 – Other 1 – Sea Transport 2 – Rail transport 3 – Road transport 4 – Air transport 5 – Postal consignment 7 – Fixed transport installations 8 – Inland waterway transport
Transport_vehicle	Identification of the vehicle (i.e. number plates, train number, plane/flight number, ship name or other identification)	Text	S	M	
Transport_container1	Indication if the transport is containerised and uses an individual transport unit code (e.g. SSCC)	Boolean	S	M	0 – No 1 – Yes
Transport_container2	Individual transport unit code of the container	ITU	S	M, if Transport_container1 = 1	
EMCS	Dispatch under the Excise Movement and Control System (EMCS)	Boolean	S	M	0 – No 1 – Yes
EMCS_ARC	Administrative Reference Code (ARC)	ARC	S	M, if EMCS = 1	
UI_Type	Identification of UI types subject to the trans-loading (recorded at the highest level of available aggregation)	Integer	S	M	1 – only unit packet level UIs 2 – only aggregated level UIs 3 – both unit packet and

Trans-loading event					
Field	Description	Data Type	Cardinality	Priority	Values
					aggregated level UIs
upUIs	List of unit packet level UIs subject to the trans-loading	upUI(L)	M	M, if UI_Type = 1 or 3	
aUIs	List of aggregated level UIs subject to the trans-loading	aUI	M	M, if UI_Type = 2 or 3	
Transloading_comment	Comments by the reporting entity	Text	S	O	

Response:

Trans-loading event – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = ETL

3.5.2.4.6. Disaggregation of aggregated level UIs event

Request:

UID application event					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = EUA
EO_ID	Economic operator's identifier	EOID	S	M	
F_ID	Facility's identifier	FID	S	M	
Event_Time	Time of event occurrence	Time(s)	S	M	
aUI	Aggregated level UI subject to disaggregation	aUI	S	M	
disaUI_comment	Comments by the reporting entity	Text	S	O	

Response:

UID application event – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = EUA

3.5.2.4.7. Report of delivery carried out with a vending van to retail outlet (required if in message type 3-3, field Destination_ID1 = 4) event

Request:

UID application event					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = EUA
EO_ID	Economic operator identifier code of the submitting entity	E OID	S	M	
F_ID	Facility identifier code of retail outlet	F ID	S	M	
Event_Time	Time of event occurrence	Time(s)	S	M	
UI_Type	Identification of UI types delivered (recorded at the highest level of available aggregation)	Integer	S	M	1 – only unit packet level UIs 2 – only aggregated level UIs 3 – both unit packet and aggregated level UIs
upUIs	List of unit packet level UIs delivered	upUI(L)	M	M, if UI_Type = 1 or 3	
aUIs	List of aggregated level UIs delivered	aUI	M	M, if UI_Type = 2 or 3	
Delivery_comment	Comments by the reporting entity	Text	S	O	

Response:

UID application event – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = EUA

3.5.2.5. Transactional event messages

3.5.2.5.1. Issuing of the Invoice event

Request:

Invoice event					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic	S	M	M_Type = EIV

Invoice event					
Field	Description	Data Type	Cardinality	Priority	Values
		Information Request >>			
EO_ID	Economic operator identifier code of the submitting entity	EOID	S	M	
Event_Time	Time of event occurrence	Time(s)	S	M	
Invoice_Type 1	Type of the invoice	Integer	S	M	1 – Original 2 – Correction 3 – Other
Invoice_Type 2	Description of the other type of the invoice	Text	S	M, if Invoice_Type1 = 3	
Invoice_Number	Number of the invoice	Text	S	M	
Invoice_Date	Date of the invoice	Date	S	M	
Invoice_Seller	Identity of the seller	EOID	S	M	
Invoice_Buyer1	Identification if the buyer is located in the EU	Boolean	S	M	0 – No 1 – Yes
Invoice_Buyer2	Identity of the buyer	EOID	S	M, if Invoice_Buyer1 = 1	
Buyer_Name	Buyer's registered legal name	Text	S	M, if Invoice_Buyer1 = 0	
Buyer_Addresses	Buyer's address – street name, house number, postal code, city	Text	S	M, if Invoice_Buyer1 = 0	
Buyer_CountryReg	Buyer's country of registration	Country	S	M, if Invoice_Buyer1 = 0	
Buyer_TAX_N	Buyer's tax registration number	Text	S	M, if Invoice_Buyer1 = 0	
First_Seller_EU	Identification if the invoice is issued by the first seller in the EU, i.e. the EU manufacturer or the importer, and the product is destined for the EU market	Boolean	S	M	0 – No 1 – Yes

Invoice event					
Field	Description	Data Type	Cardinality	Priority	Values
Product_Items_1	List of TPIDs corresponding to the product items listed on the invoice	TPID	M	M, if First_Seller_EU = 1	
Product_Items_2	List of product numbers corresponding to the product items listed on the invoice (in the same order as Product_Items_1)	PN	M	M, if First_Seller_EU = 1	
Product_Price	Net unit packet price per each pair of TPID and product number (in the same order as Product_Items_1)	Decimal	M	M, if First_Seller_EU = 1	
Invoice_Net	Total net amount of the invoice	Decimal	S	M	
Invoice_Currency	Currency of the invoice	Currency	S	M	
UI_Type	Identification of UI types covered by the invoice (recorded at the highest level of available aggregation)	Integer	S	M	1 – only unit packet level UIs 2 – only aggregated level UIs 3 – both unit packet and aggregated level UIs
upUIs	List of unit packet level UIs covered by the invoice	upUI(L)	M	M, if UI_Type = 1 or 3	
aUIs	List of aggregated level UIs covered by the invoice	aUI	M	M, if UI_Type = 2 or 3	
Invoice_comment	Comments by the reporting entity	Text	S	O	

Response:

Invoice – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = EIV

3.5.2.5.2. Issuing of the Order Number (Purchase) event

Request:

Purchase order event					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = EPO
EO_ID	Economic operator identifier code of the submitting entity	EOID	S	M	
Event_Time	Time of event occurrence	Time(s)	S	M	
Order_Number	Number of the purchase order	Text	S	M	
Order_Date	Date of the purchase order	Date	S	M	
UI_Type	Identification of UI types covered by the purchase order (recorded at the highest level of available aggregation)	Integer	S	M	1 – only unit packet level UIs 2 – only aggregated level UIs 3 – both unit packet and aggregated level UIs
upUIs	List of unit packet level UIs covered by the purchase order	upUI(L)	M	M, if UI_Type = 1 or 3	
aUIs	List of aggregated level UIs covered by the purchase order	aUI	M	M, if UI_Type = 2 or 3	
Order_comment	Description of the reason for delayed recording of the purchase order	Text	S	O	

Response:

Purchase order – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = EPO

3.5.2.5.3. Receipt of the Payment event

Request:

Payment record event					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = EPR
EO_ID	Economic operator identifier code of the submitting entity	EOID	S	M	
Event_Time	Time of event occurrence	Time(s)	S	M	
Payment_Date	Date of the payment receipt	Date	S	M	
Payment_Type	Type of payment	Integer	S	M	1 – bank transfer 2 – bank card 3 – cash 4 – other
Payment_Amount	Amount of the payment	Decimal	S	M	
Payment_Currency	Currency of the payment	Currency	S	M	
Payment_Payer1	Identification if the payer is located in the EU	Boolean	S	M	0 – No 1 – Yes
Payment_Payer2	Identity of the payer	EOID	S	M, if Payment_Payer1 = 1	
Payer_Name	Payer's registered legal name	Text	S	M, if Payment_Payer1 = 0	
Payer_Addresses	Payer's address – street name, house number, postal code and city	Text	S	M, if Payment_Payer1 = 0	
Payer_CountryReg	Payer's country of registration	Country	S	M, if Payment_Payer1 = 0	
Payer_TAX_N	Payer's tax registration number	Text	S	M, if Payment_Payer1 = 0	
Payment_Recipient	Identity of the recipient	EIOD	S	M	
Payment_Invoice	Indication if the payment corresponds to the existing invoice	Boolean	S	M	0 – No 1 – Yes

Payment record event					
Field	Description	Data Type	Cardinality	Priority	Values
Invoice_Paid	Number of the invoice paid with the payment	Text	S	M, if Payment_Invoice = 1	
UI_Type	Identification of UI types covered by the payment (recorded at the highest level of available aggregation)	Integer	S	M, if Payment_Invoice = 0	1 – only unit packet level UIs 2 – only aggregated level UIs 3 – both unit packet and aggregated level UIs
upUIs	List of unit packet level UIs covered by the payment	upUI(L)	M	M, if Payment_Invoice = 0 and UI_Type = 1 or 3	
aUIs	List of aggregated level UIs covered by the payment	aUI	M	M, if Payment_Invoice = 0 and UI_Type = 2 or 3	
Payment_comment	Comments by the reporting entity	Text	S	O	

Response:

Payment record – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = EPR

3.5.2.6. Recall messages

Notice: A recall with respect to operational and logistic events results in flagging the recalled message as cancelled but does not lead to the deletion of the existing database record.

Request:

recall – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic	S	M	M_Type = RCL

recall – request					
Field	Description	Data Type	Cardinality	Priority	Values
		Information Request >>			
EO_ID	Economic operator identifier code of the submitting entity	EOID	S	M	
Recall_CODE	Message recall code provided to the message sender in the acknowledgement of the original message to be recalled	Text	S	M	
Recall_Reason1	Reason for recalling the original message	Integer	S	M	See RecallReasonType in section 3.11.4.6
Recall_Reason2	Description of the reason for recalling the original message	Text	S	M, if Recall_Reason1 = 3 (other reason)	
Recall_Reason3	Any additional explanations on the reason for recalling the original message	Text	S	O	

Response:

recall – response					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = RCL

3.5.2.7. Data extraction messages

3.5.2.7.1. Request data extraction from the Data Storage (Primary/Surveillance)

Request:

request of data extraction – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = DRX
Query Statement	The requested search criteria	Text	S	M	This field should contain some standard query statement such as RQL

Response:

request of data extraction – response					
---------------------------------------	--	--	--	--	--

Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Resp	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = DRX
ETC	The estimated date and time of the conclusion	Timestamp(L)	S	M	

3.5.2.7.2. Retrieve extracted data from the Data Storage (Primary/ Surveillance)

Request:

retrieve extracted data – request					
Field	Description	Data Type	Cardinality	Priority	Values
BasicInfo_Req	Block of basic information elements	Component << Basic Information Request >>	S	M	M_Type = DTX
Request_CODE	The previously given identifier of the data extraction request	Text	S	M	

Response:

retrieve extracted data – response					
Field	Description	Data Type	Cardinality	Priority	Sample Values
BasicInfo_Response	Block of basic information elements	Component << Basic Information Response >>	S	M	M_Type = DTX
Result	The data result of the data extraction.	Component	S	M, if Error=0	This field shall contain the canonical data model

3.5.2.8. Mapping to ISO/IEC 19987:2015 EPCIS standard

The operational and transactional events can be mapped to events of the ISO/IEC 19987:2015 EPCIS standard. To that end, the following steps should be taken:

- Review the extension mechanisms of the abstract model layer defined in the EPCIS standard. The “Extension Points” approach is the one recommended by this Report. This approach is based on the usage of the extension points included in the data definitions, which are bound to XML data schemas, and service specifications. Thus, a new field may be added to an existing EPCIS Event Type in the Data Definition Layer. The EPCIS bindings, capture interface, and query interfaces defined in this specification are designed to permit this type of extension without requiring changes to the specification itself.
- Review the EPCIS core event types module, with a particular focus on the properties of the *ObjectEvent* and *AggregationEvent* events.
- **Extend the data definition layer.** Create a new complex custom schema that includes all the different schemas specified in sections: operational and transactional events. This new schema shall be referred to in the EPCIS

extensibility element, <<extension point>>, of the EPCIS event definition. Furthermore, the EPCIS standard provides detailed rules included for adding vendor/user-specific extensions to the schema.

- **Extend the service layer.** Create a new operation to acquire events, with the same input notation as the Capture service, but adding a new return schema that includes the Basic Information Block schema concerning the response. This will be achieved using the <<extension point>> of the service, as with the data schema above. This extension is necessary to accommodate the recall functionality into EPCIS because the EPCIS capture operation does not return any value, thus it is impossible to recall a message without any reference code received. With this capture service extension, it is possible to inform the sender of which code to refer when recalling.
- Populate the actual information in the EPCIS specific fields following the rules described hereafter:

Message Type	Description	EPCIS fields mapping
EUA	UID application	<ul style="list-style-type: none"> • <i>event type</i>= ObjectEvent • <i>eventTime</i>= timestamp in UTC format • <i>eventTimeZoneOffset</i>= <empty> • <i>action</i>=ADD • <i>bizStep</i>= <urn:epcglobal:cbv:bizstep:commissioning> • <i>extension point</i>= <UID application> schema
EPA	Aggregation of products	<ul style="list-style-type: none"> • <i>event type</i>= AggregationEvent • <i>eventTime</i>= timestamp in UTC format • <i>eventTimeZoneOffset</i>= <empty> • <i>action</i>=ADD • <i>bizStep</i>= <urn:epcglobal:cbv:bizstep:packing> • <i>extension point</i>= <Aggregation> schema for the Tracking and Tracing System
EDP	Dispatch of products	<ul style="list-style-type: none"> • <i>event type</i>= ObjectEvent • <i>eventTime</i>= timestamp in UTC format • <i>eventTimeZoneOffset</i>= <empty> • <i>action</i>= OBSERVE • <i>bizStep</i>= <urn:epcglobal:cbv:bizstep:shipping> • <i>extension point</i>= <Dispatch> schema
ERP	Reception of products	<ul style="list-style-type: none"> • <i>event type</i>=ObjectEvent • <i>eventTime</i>= timestamp in UTC format • <i>eventTimeZoneOffset</i>= <empty> • <i>action</i>= OBSERVE • <i>bizStep</i>= <urn:epcglobal:cbv:bizstep:receiving> • <i>extension point</i>= <Reception> schema
ETL	Trans-loading	<ul style="list-style-type: none"> • <i>event type</i>= ObjectEvent • <i>eventTime</i>= timestamp in UTC format • <i>eventTimeZoneOffset</i>= <empty> • <i>action</i>=OBSERVE • <i>bizStep</i>= <urn:epcglobal:cbv:bizstep:transporting> • <i>extension point</i>= <Trans-loading> schema
EIV	Invoice	<ul style="list-style-type: none"> • <i>event type</i>= ObjectEvent • <i>eventTime</i>= timestamp in UTC format

Message Type	Description	EPCIS fields mapping
		<ul style="list-style-type: none"> • <i>eventTimeZoneOffset</i>= <empty> • <i>action</i>= ADD • <i>bizStep</i>= <urn:epcglobal:cbv:bizstep:other> • <i>extension point</i>= <Invoice> schema
EPO	Purchase order	<ul style="list-style-type: none"> • <i>event type</i>=ObjectEvent • <i>eventTime</i>= timestamp in UTC format • <i>eventTimeZoneOffset</i>= <empty> • <i>action</i>= ADD • <i>bizStep</i>= <urn:epcglobal:cbv:bizstep:other> • <i>extension point</i>= < Purchase order > schema
EPR	Payment record	<ul style="list-style-type: none"> • <i>event type</i>= ObjectEvent • <i>eventTime</i>= timestamp in UTC format • <i>eventTimeZoneOffset</i>= <empty> • <i>action</i>=ADD • <i>bizStep</i>= <urn:epcglobal:cbv:bizstep:other> • <i>extension point</i>= < Payment record > schema

It should be remarked that any other EPCIS field included in the final schema will not be considered by the Tracking and Tracing System. Any relevant information for the System has to be populated in the aforementioned fields.

3.6. System users

This section presents the definition of system users, and their rights and responsibilities.

3.6.1. Definition

Data Storage system users are actors which interact at some level with the Data Storage solution. This interaction is performed through an interface that can be either a human-machine interface, a graphical interface that allows humans and machines to interact, or a machine-machine interface, that allows the communication between machines across an electronic channel.

Every system user is identified by a unique key – a user ID – and must be authenticated prior to any interaction with the system.

The interaction access control for the system users, with their rights and responsibilities regarding the system security, is presented in a role-based access control (RBAC).

RBAC is a high level model with the objective to simplify the management of granting permissions to users. This is especially necessary in situations where the number of users often reaches thousands. It takes access decisions based on two associations: 1) the association of users to roles based on the function that users assume and based on their responsibilities; and 2) the association of permissions to roles describing that a role has the permission to perform specific operations on objects. This means that it is easy to change the assignment of people to roles without changing permissions. (Feltus, Petit, & Sloman, 2010). RBAC allows protection of data integrity, since access across system features is not granted to any particular user, and it restricts access to information based on users' roles.

To define the system access control based on roles, the components of RBAC are the assignments of the relationship of a role to a list of permissions (role-permission), a role to another role (role-role) and finally a user to a role (user-role).

The following diagram presents the RBAC relationship between users, roles and system features.

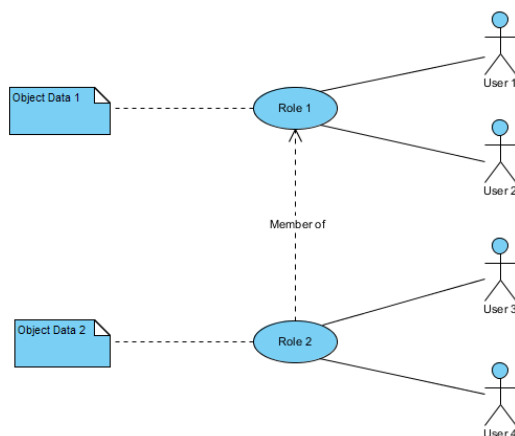


Figure 10: User-role, role-permission and role-role relationships representation

3.6.2. Responsibilities (Roles)

A role is the collection of responsibilities of a system user. It is a set of transactions that a user or set of users shall perform throughout the system processes.

The following table presents a list of potential roles related to the data storage:

System Administrator	
Description of the role	A human-machine interaction user able to maintain all system settings. The existence of at least one system administrator is paramount.
Responsibilities:	Amongst others: create, lock and unlock user accounts; grant and revoke rights to user access; ensure system availability; maintain system certificates; program system maintenance windows; network and data communication management.

Database Administrator	
Description of the user type	A human-machine interaction user able to maintain all database settings.
Responsibilities:	Amongst others: create, lock and unlock database user accounts; grant and revoke rights to data access; ensure database availability; update database versions and apply security patches; ensure the required level of database

	performance; ensure the physical database integrity; ensure the database efficiency.
--	--

System Process (background processing)	
Description of the user type	A non-human user able to perform background processing, also named batch processing, which is a pervasive workload pattern typified by bulk-oriented and non-interactive background execution. Frequently long-running, it may be data or computationally intensive, execute sequentially or in parallel, and may be initiated through various invocation models, including ad hoc, scheduled, and on-demand. (Vignola, 2013)
Responsibilities:	Non-interactive background system processing, such as process of data validation, data routing etc.

Outbound Data System Communication	
Description of the user type	A non-human user for machine-machine interaction, able to perform data extraction processes.
Responsibilities:	Tracking and tracing data extraction processing, including on-demand query execution and bulk data extraction.

Inbound Data System Communication	
Description of the user type	A non-human user for machine-machine interaction, able to perform data insertion processing.
Responsibilities:	Tracking and tracing data insertion processing.

Surveillance	
Description of the user type	A human user for human-machine interaction, able to perform data queries and extraction.
Responsibilities:	Access to the surveillance data, including on-demand query execution.

ID issuance registration	
Description of the user type	A non-human user for machine-machine interaction, able to perform data insertion processing.
Responsibilities:	ID issuance data registration processing.

Auditor	
Description of	A human user for human-machine interaction, able to perform system auditing

the user type	actions.
Responsibilities:	Direct or indirect access to the storage with wide access privileges, avoiding any mediation component to obtain system usage evidences.

3.6.3. Permissions (Rights)

The following table presents the list of potential permissions:

Permission	Description
Read System management data	Permits the reading of management data, such as system configuration, system parameters and monitoring data.
Write System management data	Permits viewing and modifying of management data, such as system configuration, system parameters, system monitoring and metrics.
Read Tracking and Tracing Related Data	Permits the reading of tracking and tracing data, such as event reporting.
Write Tracking and Tracing Related Data	Permits the writing of tracking and tracing data, such as event reporting.
Read Lookup data	Permits the reading of lookup tables, such as product identification codes and facility identification.
Write Lookup data	Permits the writing of lookup tables, such as product identification codes and facility identification.
Read ID issuance related data	Permits the reading of ID issuance related data, such as generated serial numbers.
Write ID issuance related data	Permits the writing of ID issuance related data, such as generated serial numbers.
Read system log	Permits the reading of system log, such as user activities and data manipulation.
Change own password	Permits the change of a user's own password.
Manage users	Permits the management of user configuration, creation of users, lock and unlocking of users, changing of a user password.
Multiple Logins	Permits a user to be simultaneously logged in several times.
Password expiry	Permits a user password to expire.

3.6.4. Role-permission

The following table presents the potential role-permission relationship of the system:

	System Administrator	Database Administrator	System Process (background processing)	Outbound System Communication	Inbound System Communication	Surveillance	ID issuance Registration	Auditor
Read System management data	Yes	Yes	No	No	No	No	No	Yes
Write System management data	Yes	Yes	No	No	No	No	No	No
Read Tracking and Tracing related data	No	No	Yes	Yes	No	Yes	No	Yes
Write Tracking and Tracing related data	No	No	No	No	Yes	No	No	No
Read Lookup Tables	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Write Lookup Tables	Yes	No	No	No	No	No	No	No
Read ID issuance related data	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Write ID issuance related data	No	No	No	No	No	No	Yes	No
Read system log	Yes	Yes	No	No	No	No	No	Yes
Change own password	Yes	Yes	No	No	No	Yes	No	Yes
Manage Users	Yes	Yes	No	No	No	No	No	No
Multiple logins	No	No	Yes	Yes	Yes	No	Yes	No
Password expiry	Yes	Yes	No	No	No	Yes	No	Yes

3.6.5. User-role

The following table presents the potential user-role relationship of the system:

	System Administrator	Database Administrator	System Process (background processing)	Outbound System Communication	Inbound System Communication	Surveillance	ID issuance Registration	Auditor
Competent authorities						X		
Manufacturers and importers					X			
Wholesalers and distributors					X			
ID Issuer							X	
Data Storage providers	X	X	X	X	X			
Auditors								X

3.7. Primary Data Storage

The Tracking and Tracing System is based on a **group of independent Primary Data Storage solutions**, where each Primary Data Storage **hosts data exclusively related to a specific manufacturer or importer**. As required by the TPD, this data shall be transmitted by all the economic operators involved in the trade of tobacco products, from the manufacturer to the last economic operator before the first retail outlet, and refers to the following relevant transactions of tobacco products: entry into their possession,

intermediate movements, and final exit from their possession. The Primary Data Storage solution shall also support reporting at aggregation packaging level in order to promote efficient communications, processing and storage.

Each Primary Data Storage solution shall be established by an independent third party data storage provider, which must be appointed and contracted by a specific manufacturer or importer. The Commission is responsible for approving these contracts and the selected external auditor.

Below, the requirements of the Primary Data Storage solution are specified.

3.7.1. Requirements specification

3.7.1.1. Functional

Functional Requirements – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
RQ_TTPR_FU_1	Unique identifier at unit packet level – information to be determined	Must have
<p>The Primary Data Storage solution shall ensure that the following information can be determined for a unique identifier:</p> <ul style="list-style-type: none"> • the date of manufacturing; • the place of manufacturing; • the manufacturing facility; • the machine used to manufacture the tobacco products; • the time of manufacture; • the product description; • the intended market of retail sale; • the intended shipment route; • where applicable, the importer into the Union; • the serial number; • the actual shipment route from manufacturing to the first retail outlet, including all warehouses used as well as the shipment date, shipment destination, point of departure and consignee; • the identity of all purchasers from manufacturing to the first retail outlet; and • the invoice, order number and payment records of all purchasers from manufacturing to the first retail outlet <p>This shall be accomplished through the processing of the data transmitted by the economic operators.</p>		
Source: Article 15(2) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_FU_2	Unique identifier at aggregation packaging level – information to be determined	Must have
<p>The Primary Data Storage solution shall ensure that the following information is determined for a unique identifier at aggregation packaging level:</p> <ul style="list-style-type: none"> • the date of manufacturing; • the location of the aggregation activities; and • a serial number. <p>This shall be accomplished through the processing of the data transmitted by the economic operators.</p>		
Source: Article 15(5) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_FU_3	All relevant transactions – storage	Must have
<p>The Primary Data Storage shall ensure that all relevant transactions of all natural and legal persons engaged in the supply chain of tobacco products that are received into the system are stored properly.</p>		
Source: Article 15(6) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		

Functional Requirements – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
RQ_TTPR_FU_4	All relevant transactions – support at aggregation packaging level	Must have
The Primary Data Storage shall support relevant transactions that have been recorded at aggregation packaging level.		
Source: Article 15(5) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_FU_5	All relevant transactions – transmission interface for manufacturers and importers	Must have
The Primary Data Storage shall provide a secure interface for the manufacturers and importers to allow the transmission of all relevant transactions.		
Source: Article 15(7) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_FU_6	Shipment and trade information available through an electronic link	Must have
The Primary Data Storage shall provide a secure interface to make available shipment and trade information through a link to the unique identifier.		
Source: Article 15(4) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_FU_7	Stored data - prevent data access	Must have
The Primary Data Storage shall prevent access by any party other than the competent authorities of the Member States, the Commission, and the external auditors, thereby ensuring that economic operators or any other party involved in the trade of tobacco products are forbidden to read, update or delete any data stored in the system.		
Source: Article 15(9) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_FU_8	Stored data – global copy	Must have
Once the Primary Data Storage has successfully processed and stored any relevant transaction reported from the manufacturer or importer, a copy of this same record shall be transmitted to the Surveillance Data Storage.		
Source: Article 15(6) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014), Section 3.2.4 of (everis, 2017)		
RQ_TTPR_FU_9	Recall of messages	Must have
The Primary Data Storage shall accept the recall of messages in such a way that any report transmitted by the economic operators can be recalled. There shall be no time limitation in accepting the recall of messages.		
Source: Contractor's expertise		
RQ_TTPR_FU_10	Data query – visual query tool	Must have
The Primary Data Storage shall provide a visual query tool to allow auditors, competent authorities and the Commission to make manual queries without technical knowledge of any specific query language. The queries that shall be supported by the tool are illustrated in the use case section of WP3.		
Source: Use case – Query data		
RQ_TTPR_FU_11	Data query – API query tool	Should have
The Primary Data Storage should provide an API (Application Programming Interface) query tool to allow auditors, competent authorities and the Commission to programmatically interface with the solution to query data. The queries that shall be supported by the tool are illustrated in the use case section of WP3.		

Functional Requirements – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
Source: Use case – Query data		
RQ_TTPR_FU_12	Bulk data extraction	Should have
The Primary Data Storage should provide an interface for human interaction for auditors, competent authorities and the Commission to perform bulk data extraction, using the data formats most commonly used for this purpose, such as CSV, flat file format, etc.		
Source: Use case		
RQ_TTPR_FU_13	All relevant transactions – transmission interface for the Surveillance Data Storage	Must have
The Primary Data Storage shall provide an interface to allow data exchange with the Surveillance Data Storage in order to enable the acquisition of the records transmitted by the distributors and wholesalers through the Surveillance Data Storage router.		
Source: Article 15(6) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_FU_14	System maintenance	Must have
The Primary Data Storage shall provide a user interface to allow system maintenance.		
Source: Contractor's expertise		
RQ_TTPR_FU_15	Data auditing access	Must have
The Primary Data Storage shall provide an interface to allow authorised users access to audit data.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_FU_16	Data audit trail	Must have
The Primary Data Storage shall provide a functional audit trail for every data entry.		
Source: Contractor's expertise		
RQ_TTPR_FU_17	Data access authorisation	Must have
The Primary Data Storage shall provide and limit data access to authorised users only.		
Source: Article 15(8) and 15(9) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_FU_18	Logical deletion of data	Must have
The tracking and tracing data records may only be logically deleted until the moment of the definitive data purge, in accordance with the required data retention period.		
Source: Contractor's expertise		
RQ_TTPR_FU_19	Data retention period	Must have
The Primary Data Storage shall provide a retention period of at least ten (10) years after the reception of the reported event. Data records must be kept accessible during this period.		
Source: (everis, 2017)		
RQ_TTPR_FU_20	Operations audit trail	Must have

Functional Requirements – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
<p>The Primary Data Storage shall keep audit trails (logs) for every operation performed, including any data access or manipulation. Every data change must be logged, including the original value. The audit trail shall contain at least the following information:</p> <ul style="list-style-type: none"> • Audit ID: A unique unchangeable auto-number containing the audit's key • Edit Date: A date/time containing the timestamp of the change • User: The user ID of the user who made the change • Record ID: The value that uniquely identifies the changed record • Source: The name of the object (table/view/document) that contains the changed record • Field: The name of the changed field • Before Value: The value before the change 		
Source: Contractor's expertise		
RQ_TTPR_FU_21	Lookup tables for offline verification - interface	Must have
<p>The Primary Data Storage shall provide an interface to allow offline applications to download the lookup tables to verify the unique identifier information.</p>		
Source: Contractor's expertise		
RQ_TTPR_FU_22	User authentication and authorisation	Must have
<p>The Primary Data Storage shall establish an authentication mechanism, to ensure that only authenticated users have access to the system, and an authorisation mechanism, to ensure that the authenticated user has authorisation to access the system.</p>		
Source: Contractor's expertise		
RQ_TTPR_FU_23	Change the user password	Must have
<p>The Primary Data Storage provider shall establish a mechanism to allow the user to change his/her own password.</p>		
Source: Contractor's expertise		
RQ_TTPR_FU_24	Recover the user password	Must have
<p>The Primary Data Storage provider shall establish a mechanism to allow the user to recover his/her own password.</p>		
Source: Contractor's expertise		
RQ_TTPR_FU_25	Deactivate user	Must have
<p>The Primary Data Storage provider shall establish a mechanism to allow System Administrators to deactivate a user.</p>		
Source: Contractor's expertise		
RQ_TTPR_FU_26	Re-activate user	Must have
<p>The Primary Data Storage provider shall establish a mechanism to allow System Administrators to re-activate a user.</p>		
Source: Contractor's expertise		
RQ_TTPR_FU_27	Provisioning of additional capabilities laid down in future updates of the Implementing Acts	Must have
<p>The Primary Data Storage provider shall accommodate any additional capability or system update that could be laid down in future amendments to the relevant EU legislation.</p>		

Functional Requirements – Tracking and Tracing System – Primary Data Storage

ID	Name	Priority
Source: Contractor's expertise		

3.7.1.2. Technical

3.7.1.2.1. System qualities

System Qualities – Tracking and Tracing System – Primary Data Storage

ID	Name	Priority
RQ_TTPR_RE_1	Data reception acknowledgment	Must have
The Primary Data Storage shall acknowledge the sender of a successful data receipt, otherwise failing with a consistent error code.		
Source: Contractor's expertise		
RQ_TTPR_RE_2	Business continuity and disaster recovery	Must have
The Primary Data Storage provider shall provide data resilience and disaster recovery capabilities across multiple sites.		
Source: Contractors' expertise		
RQ_TTPR_RE_3	Data backups	Must have
The Primary Data Storage provider shall take periodic full and/or incremental snapshots of the data store to mitigate the risk of system/storage failure.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_RE_4	Outbound channel redundancy	Must have
The Primary Data Storage shall be able to change automatically to additional outbound communication channels (at least one shall be established) in case the message submission fails due to a communication error with the Surveillance Data Storage.		
Source: Contractor's expertise		
RQ_TTPR_RE_5	Message replay-ability	Must have
The Primary Data Storage shall persist the outgoing messages until the messages are successfully delivered. When trying to transmit the outgoing messages, the Primary Data Storage shall handle transient failures by transparently retrying a failed operation.		
Source: Contractor's expertise		
RQ_TTPR_PE_1	Storage size	Must have
The Primary Data Storage shall be able to support storage size of at least 25 Terabytes per instance yearly.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014), (everis,		

System Qualities – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
2017)		
RQ_TTPR_PE_2	Messaging throughput	Must have
The Primary Data Storage shall support rates of message throughput for input/output operations in the range of fifty thousand (50,000) messages per second per instance.		
Source: (everis, 2017)		
RQ_TTPR_PE_3	Query request throughput	Must have
The Primary Data Storage shall be able to support at least five hundred (500) concurrent query requests per instance.		
Source: (everis, 2017)		
RQ_TTPR_PE_4	Network uptime	Must have
The Primary Data Storage facility shall be able to meet the network uptime target: 99.5% (Tier III data centre).		
Source: Contractor's expertise		
RQ_TTPR_PE_5	Server uptime	Must have
The Primary Data Storage facility shall be able to meet the server uptime target: 99.5% (Tier III data centre).		
Source: Contractor's expertise		
RQ_TTPR_PE_6	Latency intra data centre	Must have
The Primary Data Storage facility shall be able to meet the latency target: less than 100 milliseconds latency between physical servers in the same data centre.		
Source: Contractor's expertise		
RQ_TTPR_PE_7	Inter data centre speed	Must have
The Primary Data Storage facility shall be able to meet the speed target: at least 100 Mbps between the different data centres involved, namely the Surveillance Data Storage solution and ID Issuer solutions.		
Source: Contractor's expertise		
RQ_TTPR_PE_8	Support response time	Must have
The Primary Data Storage provider shall be able to meet the support response time target: 30 minute support response time for emergency incidents.		
Source: Contractor's expertise		
RQ_TTPR_PE_9	Hardware break/fix	Must have
The Primary Data Storage provider shall be able to meet the hardware break/fix target: subject to the vendor-backed support.		
Source: Contractor's expertise		
RQ_TTPR_PE_10	Data archiving	Must have
The Primary Data Storage provider shall securely archive data that is no longer required by the system, in compliance with the required retention period, thus reducing the size of the data store.		

System Qualities – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
Source: Contractor's expertise		
RQ_TTPR_PE_11	Separate physical data storage areas	Must have
The Primary Data Storage provider shall create a tiered storage environment utilising multiple media types delivering the required combinations of performance, capacity and resilience.		
Source: (European Commission - JRC, 2017)		
RQ_TTPR_PE_12	Data centre efficiency	Should have
The Primary Data Storage provider should be compliant with the European Code of Conduct for Energy Efficiency in Data Centres, and use best practices for data centre energy efficiency.		
Source: (European Commission - JRC, 2017)		
RQ_TTPR_SU_1	Scalability	Must have
The Primary Data Storage facility shall be scalable and technically upgradeable to maintain performance against threat growth. This includes I/O performance, storage and network capacity, and licences.		
Source: Contractor's expertise		
RQ_TTPR_SU_2	Unlimited by design	Must have
The Primary Data Storage shall have growth potential beyond the figures given in this section in order to host all relevant data for at least the totality of the retention period. Therefore, the data storage capacity and the database size shall not deem any limitation on design.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_SU_3	Notification of storage limit	Must have
The Primary Data Storage provider shall notify the system administrator and the correspondent manufacturer or importer when the allocated storage reaches 75% of its total capacity.		
Source: Contractor's expertise		
RQ_TTPR_SU_4	Support to connectivity tests with economic operators connectivity	Must have
The Primary Data Storage provider shall provide the manufacturer or importer, which has established this repository, with the necessary support (e.g. credentials, configuration information, documentation, sample data, test sets, etc.) to verify the compliance of his event reporting components (e.g. Temporary Buffer) with the system requirements prior to the connection to production.		
Source: Contractor's expertise		
RQ_TTPR_SU_5	Operational support to economic operators	Must have
The Primary Data Storage provider shall provide to the manufacturer or importer, which has established this repository, the necessary operational support (e.g. credentials, configuration information, documentation, sample data, connectivity verification, issues monitoring, test sets, etc.) to facilitate a smooth production functioning of his reporting components (e.g. Temporary Buffer).		
Source: Contractor's expertise		
RQ_TTPR_SU_6	Support to connectivity tests with the Surveillance Data Storage solution	Must have
The Primary Data Storage provider shall provide to the Surveillance Data Storage provider the necessary support (e.g. credentials, configuration information, documentation, sample data, test sets, etc.) to verify the compliance of his implementation with the system requirements prior to the connection to production.		
Source: Contractor's expertise		

System Qualities – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
RQ_TTPR_SU_7	Operational support to Surveillance Data Storage solution	Must have
The Primary Data Storage provider shall provide to the Surveillance Data Storage provider the necessary support (e.g. credentials, configuration information, documentation, sample data, connectivity verification, issues monitoring, test sets, etc.) to facilitate a smooth production functioning of both solutions.		
Source: Contractor's expertise		
RQ_TTPR_SU_8	Support to interface versioning	Must have
The Primary Data Storage provider shall support any data model or functionality evolution through the release of a new interface version in accordance with the new features.		
Source: Contractor's expertise		

3.7.1.2.2. Security

Security – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
RQ_TTPR_SE_1	Data isolation	Must have
The Primary Data Storage provider shall provide economic operators with a secure and segmented hosting environment with server, storage, and network elements that are logically isolated from other economic operators running on the same infrastructure.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_SE_2	User access authorisation	Must have
The Primary Data Storage shall provide a user authorisation mechanism in order to ensure the segregation of responsibilities and restrict access to data.		
Source: Article 15(7) and 15(9) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_SE_3	Auditability	Must have
The Primary Data Storage provider shall provide auditing, an audit trail with change recording, and an activity logging mechanism with timestamps for all data-related activities.		
Source: Article 15(8) (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_SE_4	Audit logging	Must have
The Primary Data Storage shall record important events together with the user who performs the operation in an audit log, which shall be centrally maintained. The list of events that the Primary Data Storage shall record in the audit log shall include but not be limited to the following: <ul style="list-style-type: none"> • Database activities • Technical events, like data synchronisation and data replication • Accessing of data 		
Source: Contractor's expertise		
RQ_TTPR_SE_5	Error logging	Must have
All errors and faults in the Primary Data Storage shall be recorded in an error log, which shall be centrally maintained.		

Security – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
Source: Contractor's expertise		
RQ_TTPR_SE_6	Completeness of logs	Must have
The error log and audit log shall contain all required information in order to provide the authorised user with interpretable and comprehensive information about the cause of the error, as well as the audit traceability for the actions taken by an authorised user.		
Source: Contractor's expertise		
RQ_TTPR_SE_7	Auditing and monitoring plan	Must have
The Primary Data Storage provider shall implement an auditing and monitoring plan. The plan shall address, but not be limited to, the following topics: <ul style="list-style-type: none"> • Auditing of vulnerabilities and threats • Auditing of data access • Auditing of database baseline • Monitoring of suspicious activities • Monitoring of systems health • Anomalies detection • Implementation of server hardening guidelines for securing the system 		
Source: Use case – Auditing of Data Storage		
RQ_TTPR_SE_8	End-to-end traceability	Must have
The Primary Data Storage shall ensure that any data/action can always be traced to its original source (i.e. reporting facility of manufacturer/importer/distributor/wholesaler).		
Source: Contractor's expertise		
RQ_TTPR_SE_9	Auditor support	Must have
The Primary Data Storage provider shall provide full access and any requested evidence to the independent external auditor to ensure that s/he can monitor the activities of the Primary Data Storage provider and the accesses to the Primary Data Storage solution.		
Source: Article 15(8) (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_SE_10	Log preservation	Must have
The Primary Data Storage shall archive the error and audit logs, using integrity checking countermeasures to ensure that the log file has been archived successfully after each archiving process.		
Source: Contractor's expertise		
RQ_TTPR_SE_11	Log retention period	Must have
Access logs shall be immutable and kept for at least four (4) years. Error logs shall be immutable and kept for at least two (2) years.		
Source: Contractor's expertise		
RQ_TTPR_SE_12	Sender tracking	Must have
The Primary Data Storage shall resolve and authenticate the sender's identity against a trusted identity provider. Messages sent from an unauthenticated sender shall not be accepted.		
Source: Contractor's expertise		

Security – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
RQ_TTPR_SE_13	Checksum verification	Must have
The Primary Data Storage shall verify the message checksum to ensure that the data was not tampered with. Messages where the checksum is not valid shall not be accepted.		
Source: Contractor's expertise		
RQ_TTPR_SE_14	Secure coding practice	Must have
The Primary Data Storage provider shall provide a system implementation compliant with common secure coding practices, such as OWASP.		
Source: Contractor's expertise		
RQ_TTPR_SE_15	User access authentication	Must have
The Primary Data Storage shall provide a user authentication mechanism prior to any access to system resources and data.		
Source: Contractor's expertise		
RQ_TTPR_SE_16	Password strength	Must have
The Primary Data Storage shall ensure the enforcement of password standards (e.g. minimum length and use of alpha, numeric and special characters) and, when applicable, establish a specified period for password expiration and prohibit the user from reusing recent passwords.		
Source: Contractor's expertise		
RQ_TTPR_SE_17	Password protection	Must have
The Primary Data Storage shall ensure that user passwords are non-printing and non-displaying.		
Source: Contractor's expertise		
RQ_TTPR_SE_18	Integration with the European single sign-on mechanism	Should have
The Primary Data Storage should provide integration with the European access control mechanism (i.e. "EU Login") to allow competent authorities to use a single sign-on to the system, when applicable.		
Source: Contractor's expertise		

3.7.1.2.3. Data protection

Data Protection – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
RQ_TTPR_DP_1	Data protection rules	Must have
The Primary Data Storage provider shall be compliant with and ensure that personal data is processed and protected in accordance with EU Regulation 2016/679 (European Commission - REGULATION (EU) 2016/679, 2016), which repeals Directive 95/46/EC.		
Source: Article 15(10) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_DP_2	Antitrust	Must have

Data Protection – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
The data confidentiality must follow all the necessary safeguarding measures, respecting the current ruling of antitrust, in order to prevent the leak or access of any sensitive data of an economic operator by any other economic operator.		
Source: Contractor's expertise		
RQ_TTPR_DP_3	Confidentiality treatment	Must have
The Primary Data Storage provider must treat with confidentiality any information, or documents disclosed, in any format exchanged or stored in the system.		
Source: Contractor's expertise		

3.7.1.2.4. System constraints

System Constraints – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
RQ_TTPR_SC_1	Facility location	Must have
The Primary Data Storage facility shall be physically located within the territory of the European Union, and any maintenance on the servers shall be carried out within the European Union.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_SC_2	Extension of guarantees	Must have
Any additional exchange of data and metadata that might occur in the Primary Data Storage facility with the objective to implement or support the Tracking and Tracing System shall be guaranteed the same level of data protection and quality as defined for the rest of the system.		
Source: Contractor's expertise		
RQ_TTPR_SC_3	Non-limiting throughput for economic operators	Must have
The overall throughput of the Primary Data Storage shall not be a limiting factor for the speed of the manufacturing production lines or for the logistics activities of importers, distributors or wholesalers.		
Source: Contractor's expertise		
RQ_TTPR_SC_4	Data dictionary compatibility	Must have
The Primary Data Storage solution shall ensure that the physical storage of the Tracking and Tracing data is conformant with the data dictionary described in section 3.11.		
Source: Contractor's expertise		
RQ_TTPR_SC_5	Data validation rules	Must have
The Primary Data Storage solution shall implement Tracking and Tracing data validation rules conformant with the common validation rules described in section 3.12.		
Source: Contractor's expertise		

System Constraints – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
RQ_TTPR_SC_6	Messaging compatibility	Must have
The Primary Data Storage solution shall exchange messages conformant with the specifications described in section 3.5.1.		
Source: Contractor's expertise		
RQ_TTPR_SC_7	Decoupling of operations	Must have
The Primary Data Storage must decouple data acquisition from data processing, avoiding unnecessary coupling between independent processes.		
Source: Contractor's expertise		
RQ_TTPR_SC_8	Event-driven design	Must have
The Primary Data Storage shall be designed based on an event-driven architectural pattern for the data acquisition and data processing components.		
Source: Contractor's expertise		
RQ_TTPR_SC_9	Fault isolation	Must have
The main components of the Primary Data Storage shall be designed to support fault isolation, in order to not propagate its errors to other components of the solution and to limit the impact of any problem to the minimum.		
Source: Contractor's expertise		
RQ_TTPR_SC_10	Designed for monitoring	Must have
The Primary Data Storage solution shall be designed for monitoring in order to help the provider in the identification of current, potential or future issues (e.g. performance, code bugs, application errors, security threats, etc.). The monitoring should be applied at the following levels: hardware, software, infrastructure and application (the latter aiming at reporting on "what is the problem").		
Source: Contractor's expertise		
RQ_TTPR_SC_11	Idempotent messages	Must have
The Primary Data Storage message management shall be designed to avoid acquiring and reprocessing the same message multiple times, since messages of the Tracking and Tracing System are not idempotent.		
Source: Contractor's expertise		
RQ_TTPR_SC_12	Usage of an agnostic query language to retrieve the canonical data model	Should have
The Primary Data Storage should provide an interface compliant with some agnostic query language to retrieve data from the Tracking and Tracing canonical data model. As such, the Resource Query Language (RQL), which is an open language (apsstandard - RQL, 2014) for querying collections of resources, could be a potential solution.		
Source: Contractor's expertise		

3.7.1.2.5. System interfaces

Interface PR2MI

ID	Name
▪ PR2MI	▪ Primary Data Storage to manufacturers and importers
Owner System	
▪ Primary Data Storage solution	
Data Source	Data Target
▪ Component established at the facilities of the manufacturers or importers to report events	▪ Primary Data Storage
Data Type	
<ul style="list-style-type: none"> ▪ Operational event messages ▪ Transactional event messages 	
Interface Trigger	
▪ Push upon request by the client systems of the economic operators.	
Access Control	
▪ Only authorised manufacturers and importers have access to this interface.	
Description	
▪ This interface provides the event information reporting channel to the manufacturers and importers.	

Interface PR2CA	
ID	Name
▪ PR2CA	▪ Primary Data Storage to competent authorities
Owner System	
▪ Primary Data Storage solution	
Data Source	Data Target
▪ Primary Data Storage	▪ Competent authorities
Data Type	
<ul style="list-style-type: none"> ▪ Operational event messages ▪ Transactional event messages ▪ Data extraction messages ▪ Lookup tables ▪ Notifications 	
Interface Trigger	
▪ Push execution on demand.	
Access Control	
▪ Only the competent authorities have access to this interface.	

Description
<ul style="list-style-type: none"> ▪ This interface provides the channel to give competent authorities full access to the Primary Data Storage.

Interface PR2AU	
ID	Name
<ul style="list-style-type: none"> ▪ PR2AU 	<ul style="list-style-type: none"> ▪ Primary Data Storage to auditors
Owner System	
<ul style="list-style-type: none"> ▪ Primary Data Storage solution 	
Data Source	Data Target
<ul style="list-style-type: none"> ▪ Primary Data Storage 	<ul style="list-style-type: none"> ▪ Auditors
Data Type	
<ul style="list-style-type: none"> ▪ Operational event messages ▪ Transactional event messages ▪ Data extraction messages ▪ Lookup tables ▪ Notifications 	
Interface Trigger	
<ul style="list-style-type: none"> ▪ Pull execution on demand. 	
Access Control	
<ul style="list-style-type: none"> ▪ Only the auditors have access to this interface. 	
Description	
<ul style="list-style-type: none"> ▪ This interface provides the channel to give auditors access to the auditing data of the Primary Data Storage. 	

Interface PR2SU	
ID	Name
<ul style="list-style-type: none"> ▪ PR2SU 	<ul style="list-style-type: none"> ▪ Primary Data Storage to Surveillance Data Storage
Owner System	
<ul style="list-style-type: none"> ▪ Primary Data Storage solution 	
Data Source	Data Target
<ul style="list-style-type: none"> ▪ Surveillance Data Storage 	<ul style="list-style-type: none"> ▪ Primary Data Storage
Data Type	
<ul style="list-style-type: none"> ▪ Operational event messages ▪ Transactional event messages ▪ Replication of lookup tables 	

Interface Trigger
▪ Push execution on demand.
Access Control
▪ Only the Surveillance Data Storage has access to this interface.
Description
▪ This interface provides the channel to the Repository Router to update the Primary Data Storage.

3.7.1.3. Applicable standards

Applicable Standards – Tracking and Tracing System – Primary Data Storage		
ID	Name	Priority
RQ_TTPR_AS_1	ISO 27001 compliant hosting	Must have
The Primary Data Storage shall be hosted in an ISO 27001 compliant hosting. This provider is expected to deliver a highly available, scalable, and flexible system.		
Source: Contractor’s expertise		
RQ_TTPR_AS_2	Character set content	Must have
The Primary Data Storage shall store content using the ISO/IEC 8859-15:1999 character set.		
Source: Contractor’s expertise		

3.8. Surveillance Data Storage

The Tracking and Tracing System also includes a central **Surveillance Data Storage solution**, which hosts a **global copy** of the distributed data. On this basis, the Surveillance Data Storage solution is in a position to offer a **comprehensive logical view** of all relevant data based on local data, which could be further exploited through analytic capabilities (e.g. risk based analytics, suspicious pattern detection, etc.) to increase the efficiency and effectiveness of national enforcement activities. In addition, this central Surveillance Data Storage solution provides a secure Repository Routing component to facilitate the seamless transmission of events reported by distributors and wholesalers through a single point.

In this particular case, the third party providers of the Primary Data Storage solutions will jointly select the third party data storage provider that will establish the Surveillance Data Storage solution.

Below, the requirements of the Surveillance Data Storage solution are specified.

3.8.1. Requirements specification

3.8.1.1. Functional

Functional Requirements – Tracking and Tracing System – Surveillance Data Storage

ID	Name	Priority
RQ_TTSU_FU_1	Unique identifier at unit packet level – information to be determined	Must have
<p>The Surveillance Data Storage solution shall ensure that the following information is determined for a unique identifier at unit packet level:</p> <ul style="list-style-type: none"> • the place of manufacturing; • the manufacturing facility; • the machine used to manufacture the tobacco products; • the date of manufacturing; • the time of manufacture or production shift; • the product description; • the intended market of retail sale; • the intended shipment route; • where applicable, the importer into the Union; • the serial number; • the actual shipment route from manufacturing to the first retail outlet, including all warehouses used as well as the shipment date, shipment destination, point of departure and consignee; • the identity of all purchasers from manufacturing to the first retail outlet; and • the invoice, order number and payment records of all purchasers from manufacturing to the first retail outlet <p>This shall be accomplished through the processing of the data transmitted by the economic operators.</p>		
Source: Article 15(2) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_FU_2	Unique identifier at aggregation packaging level – information to be determined	Must have
<p>The Surveillance Data Storage solution shall ensure that the following information is determined for a unique identifier at aggregation packaging level:</p> <ul style="list-style-type: none"> • the date of manufacturing; • the location of the aggregation activities; and • a serial number. <p>This shall be accomplished through the processing of the data transmitted by the economic operators.</p>		
Source: Article 15(5) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_FU_3	All relevant transactions – global copy	Must have
<p>The Surveillance Data Storage shall ensure that all relevant transactions of all natural and legal persons engaged in the supply chain of tobacco products that are received into the Tracking and Tracing System are stored properly.</p>		
Source: Article 15(6) (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_FU_4	All relevant transactions – support at aggregation packaging level	Must have
<p>The Surveillance Data Storage shall support relevant transactions that have been recorded at aggregation packaging level.</p>		
Source: Article 15(5) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_FU_5	All relevant transactions – transmission interface for Primary Data Storage	Must have
<p>The Surveillance Data Storage shall provide a secure interface to the Primary Data Storages to allow the transmission of all relevant transactions reported from manufacturers and importers.</p>		
Source: Article 15(6) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_FU_6	Shipment and trade information available through an electronic link	Must have
<p>The Surveillance Data Storage shall provide a secure interface to make available shipment and trade information through a link to the unique identifier.</p>		
Source: Article 15(4) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		

Functional Requirements – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
RQ_TTSU_FU_7	All relevant transactions – transmission interface for distributors and wholesalers	Must have
The Surveillance Data Storage shall provide a secure interface to distributors and wholesalers to allow the transmission of all relevant transactions reported from such sources.		
Source: Article 15(6) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_FU_8	All relevant transactions – routing of distributors and wholesalers records	Must have
The Surveillance Data Storage shall provide a routing service for the records transmitted by the distributors and wholesalers, which shall also be processed by the manufacturers/importers that they refer to.		
Source: Article 15(6) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_FU_9	Stored data - prevent data access	Must have
The Surveillance Data Storage shall prevent access by any party other than the competent authorities of the Member States, the Commission, and the external auditors, thereby ensuring that economic operators or any other party involved in the trade of tobacco products are forbidden to read, update or delete any data stored in the system.		
Source: Article 15(9) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_FU_10	Recall of messages	Must have
The Surveillance Data Storage shall accept the recall of messages in such a way that any report transmitted by the economic operators can be recalled. There shall be no time limitation in accepting the recall of messages.		
Source: Contractor's expertise		
RQ_TTSU_FU_11	Data query – visual query tool	Must have
The Surveillance Data Storage shall provide a visual query tool to allow auditors and competent authorities to make manual queries without technical knowledge of any specific query language. The queries that shall be supported by the tool are illustrated in the use case section of WP3.		
Source: Use case – Query data		
RQ_TTSU_FU_12	Data query – API query tool	Should have
The Surveillance Data Storage should provide an API (Application Programming Interface) query tool to allow auditors and competent authorities to programmatically interface with the solution to query data. The queries that shall be supported by the tool are illustrated in the use case section of WP3.		
Source: Use case – Query data		
RQ_TTSU_FU_13	Bulk data extraction	Should have
The Surveillance Data Storage should provide an interface for human interaction for auditors, competent authorities, and the Commission to perform bulk data extraction for further analysis, using the data formats most commonly used for this purpose, such as CSV, flat file format, etc.		
Source: Contractor's expertise		
RQ_TTSU_FU_14	Data query – data grouping	Must have
The Surveillance Data Storage shall provide the capability to perform queries, retrieving any information containing data aggregation, such as grouping and having.		
Source: Contractor's expertise		

Functional Requirements – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
RQ_TTSU_FU_15	Data query – data calculation	Must have
The Surveillance Data Storage shall provide the capability to perform queries, retrieving any information that is calculated and not stored, such as sums or averages.		
Source: Contractor’s expertise		
RQ_TTSU_FU_16	Data query – data sorting	Must have
The Surveillance Data Storage shall provide the capability to perform queries, retrieving sorted information.		
Source: Contractor’s expertise		
RQ_TTSU_FU_17	Lookup tables - data maintenance	Must have
The Surveillance Data Storage shall provide a mechanism to allow the maintenance of the lookup tables.		
Source: Contractor’s expertise		
RQ_TTSU_FU_18	System maintenance	Must have
The Surveillance Data Storage shall provide a user interface to allow system maintenance.		
Source: Contractor’s expertise		
RQ_TTSU_FU_19	Auditing data access	Must have
The Surveillance Data Storage shall provide an interface to allow access to audit data.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_FU_20	Data audit trail	Must have
The Surveillance Data Storage shall provide a functional audit trail for every data entry.		
Source: Contractor’s expertise		
RQ_TTSU_FU_21	Data access authorisation	Must have
The Surveillance Data Storage shall provide and limit data access to authorised users only.		
Source: Article 15(8) and 15(9) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_FU_22	Logical deletion of data	Must have
The Tracking and Tracing data records may only be logically deleted until the moment of the definitive data purge, in accordance with the required data retention period.		
Source: Contractor’s expertise		
RQ_TTSU_FU_23	Data retention period	Must have
The Surveillance Data Storage shall provide a retention period of at least ten (10) years after the reception of the reported event. Data records must be kept accessible during this period.		

Functional Requirements – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
Source: (everis, 2017)		
RQ_TTSU_FU_24	Operations audit trail	Must have
<p>The Surveillance Data Storage shall provide and keep audit trails (logs) for every operation performed, including any data access or manipulation. Every data change must be logged, including the original value. The audit trail shall contain at least the following information:</p> <ul style="list-style-type: none"> • Audit ID: a unique unchangeable auto-number containing the audit key • Edit Date: A date/time containing the timestamp of the change • User: The ID of the user that made the change • Record ID: The value that uniquely identifies the changed record • Source: The name of the object (table/view/document) that contains the changed record • Field: The name of the changed field • Before Value: The value before the change 		
Source: Contractor's expertise		
RQ_TTSU_FU_25	Lookup tables for offline verification - interface	Must have
<p>The Surveillance Data Storage shall provide an interface to allow offline applications to download the lookup tables and verify the unique identifier information.</p>		
Source: Contractor's expertise		
RQ_TTSU_FU_26	User authentication and authorisation	Must have
<p>The Surveillance Data Storage shall establish an authentication mechanism to ensure that only authenticated users have access to the system, and an authorisation mechanism, to ensure that the authenticated user has authorisation prior to any system access.</p>		
Source: Contractor's expertise		
RQ_TTSU_FU_27	Change the user password	Must have
<p>The Surveillance Data Storage provider shall establish a mechanism to allow the user to change his/her own password.</p>		
Source: Contractor's expertise		
RQ_TTSU_FU_28	Recover the user password	Must have
<p>The Surveillance Data Storage provider shall establish a mechanism to allow the user to recover his/her own password.</p>		
Source: Contractor's expertise		
RQ_TTSU_FU_29	Deactivate user	Must have
<p>The Surveillance Data Storage provider shall establish a mechanism to allow System Administrators to deactivate a user.</p>		
Source: Contractor's expertise		
RQ_TTSU_FU_30	Re-activate user	Must have
<p>The Surveillance Data Storage provider shall establish a mechanism to allow System Administrators to re-activate a user.</p>		
Source: Contractor's expertise		

Functional Requirements – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
RQ_TTSU_FU_31	Data analytics capabilities	Must have
The Surveillance Data Storage shall provide data analytics capabilities in order to provide information tools to support national enforcement activities and the Commission. Each authorised user (i.e. competent authorities and the Commission) shall have his/her own data analytics environment in which to configure his/her own rules. See the risk-based surveillance use case for further details.		
Source: Use case – Risk-based surveillance		
RQ_TTSU_FU_32	Key indicators tool	Could have
The Surveillance Data Storage could provide a tool acting as a dashboard, where key indicators of the system could be configured.		
Source: Contractor’s expertise		
RQ_TTSU_FU_33	Notification tool	Must have
The Surveillance Data Storage shall provide a tool for automatic notifications to be triggered based on configurable parameters and criteria. The tool should provide the possibility of configuring different notification channels and recipient stakeholders. Each authorised user (i.e. competent authorities and the Commission) shall have his/her own environment in which to configure his/her own notifications and channels. See the notify use case for further details.		
Source: Use case - Notify		
RQ_TTSU_FU_34	Query notification	Must have
The Surveillance Data Storage shall provide a visual interface to allow competent authorities, external auditors, and the Commission to query notifications generated.		
Source: Contractor’s expertise		
RQ_TTSU_FU_35	Control access of data extraction	Must have
The Surveillance Data Storage shall ensure that any data extraction shall be compliant with the data access level of the requestor.		
Source: Contractor’s expertise		
RQ_TTSU_FU_36	Data view format	Must have
The Surveillance Data Storage shall provide the capability to present data in a row and column format, with information vertically listed in column-by-column headings and in horizontal bands, and with each band having its own content possibly spanning multiple lines.		
Source: Contractor’s expertise		
RQ_TTSU_FU_37	Data drill down	Should have
The Surveillance Data Storage should provide the capability to present data at specific level, and drill down to other levels of information for a selected value (e.g. Pallet > Master Case > Carton > Unit Packet).		
Source: Contractor’s expertise		
RQ_TTSU_FU_38	Data drill up	Should have
The Surveillance Data Storage should provide the capability to present data at specific level, and drill up to other levels of information for a selected value (e.g. Unit Packet > Carton > Master Case > Pallet).		

Functional Requirements – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
Source: Contractor’s expertise		
RQ_TTSU_FU_39	Provisioning of additional capabilities laid down in future updates of the Implementing Acts	Must have
The Surveillance Data Storage provider shall accommodate any additional capability or system update laid down in future amendments to the relevant legislation.		
Source: Contractor’s expertise		

3.8.1.2. Technical

3.8.1.2.1. System qualities

System Qualities – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
RQ_TTSU_RE_1	Data reception acknowledgment	Must have
The Surveillance Data Storage shall send acknowledgement of a successful data receipt to the sender, otherwise failing with a consistent error code.		
Source: Contractor’s expertise		
RQ_TTSU_RE_2	Business continuity and disaster recovery	Must have
The Surveillance Data Storage provider shall provide data resilience and disaster recovery capabilities across multiple sites.		
Source: Contractors’ expertise		
RQ_TTSU_RE_3	Data backups	Must have
The Surveillance Data Storage provider shall take periodic full and/or incremental snapshots of the data store to mitigate the risk of system/storage failure.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTPR_RE_4	Outbound channel redundancy	Must have
The Surveillance Data Storage shall be able to change automatically to additional outbound communication channels (at least one shall be established) in case the message submission fails due to a communication error with the Primary Data Storage.		
Source: Contractor’s expertise		
RQ_TTSU_PE_1	Storage size	Must have
The Surveillance Data Storage shall be able to support a storage size of at least 100 Terabytes per instance yearly.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014), (everis, 2017)		
RQ_TTSU_PE_2	Messaging throughput	Must have
The Surveillance Data Storage shall support rates of message throughput for input/output operations in the range of 750 thousand (750,000) messages per second per instance.		

System Qualities – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
Source: (everis, 2017)		
RQ_TTSU_PE_3	Query request throughput	Must have
The Surveillance Data Storage shall be able to support at least five hundred (500) concurrent query requests per instance.		
Source: (everis, 2017)		
RQ_TTSU_PE_4	Network uptime	Must have
The Surveillance Data Storage facility shall be able to meet the network uptime target: 99.55% (Tier III data centre).		
Source: Contractor's expertise		
RQ_TTSU_PE_5	Server uptime	Must have
The Surveillance Data Storage facility shall be able to meet the server uptime target: 99.55% (Tier III data centre).		
Source: Contractor's expertise		
RQ_TTSU_PE_6	Latency intra data centre	Must have
The Surveillance Data Storage facility shall be able to meet the Latency Target: Less than 100 millisecond latency between physical servers in the same data centre.		
Source: Contractor's expertise		
RQ_TTSU_PE_7	Inter data centre speed	Must have
The Surveillance Data Storage facility shall be able to meet the Speed Target: more than 100 Mbps between the different data centres involved, namely the ID Issuer solutions and Primary Data Storage solutions.		
Source: Contractor's expertise		
RQ_TTSU_PE_8	Support Response Time	Must have
The Surveillance Data Storage provider shall be able to meet the support response time target: 30 minute support response time for emergency incidents.		
Source: Contractor's expertise		
RQ_TTSU_PE_9	Hardware break/fix	Must have
The Surveillance Data Storage provider shall be able to meet the hardware break/fix target: subject to the vendor-backed support.		
Source: Contractor's expertise		
RQ_TTSU_PE_10	Data archiving	Must have
The Surveillance Data Storage provider shall archive data that is no longer required by the system, in compliance with the maximum retention period required, thereby reducing the size of the data store.		
Source: Contractor's expertise		
RQ_TTSU_PE_11	Separate physical data storage areas	Must have
The Surveillance Data Storage provider shall create a tiered storage environment utilising multiple media types delivering the required combinations of performance, capacity and resilience.		

System Qualities – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
Source: (European Commission - JRC, 2017)		
RQ_TTSU_PE_12	Data centre efficiency	Should have
The Surveillance Data Storage provider should be compliant with the European Code of Conduct for Energy Efficiency in Data Centres, and use best practices for data centre energy efficiency.		
Source: (European Commission - JRC, 2017)		
RQ_TTSU_SU_1	Scalability	Must have
The Surveillance Data Storage facility shall be scalable and technically upgradeable to maintain performance against threat growth. This includes I/O performance, storage and network capacity, and licences.		
Source: Contractor's expertise		
RQ_TTSU_SU_2	Unlimited by design	Must have
The Surveillance Data Storage shall have growth potential beyond the figures given in this section to indicate data storage capacity, database or list sizes, and shall not deem any limitation on design.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_SU_3	Notification of storage limit	Must have
The Surveillance Data Storage provider shall notify the authorised user when the allocated storage reaches 75% of its total capacity.		
Source: Contractor's expertise		
RQ_TTSU_SU_4	Support to connectivity tests with economic operators	Must have
The Surveillance Data Storage provider shall provide the distributors and wholesalers with the necessary support (e.g. credentials, configuration information, documentation, sample data, etc.) to verify the compliance with the system requirements of their event reporting components (e.g. Temporary Buffer) prior to the connection to production.		
Source: Contractor's expertise		
RQ_TTSU_SU_5	Operational support to economic operators	Must have
The Surveillance Data Storage provider shall provide the distributors and wholesalers with the necessary operational support (e.g. credentials, configuration information, documentation, sample data, connectivity verification, issues monitoring, test sets, etc.) to facilitate a smooth production functioning of their reporting components (e.g. Temporary Buffer).		
Source: Contractor's expertise		
RQ_TTSU_SU_6	Support to connectivity tests with the Primary Data Storage solutions	Must have
The Surveillance Data Storage provider shall provide the different Primary Data Storage providers with the necessary support (e.g. credentials, configuration information, documentation, sample data, test sets, etc.) to verify compliance of their client implementations with the system requirements prior to the connection to production.		
Source: Contractor's expertise		
RQ_TTSU_SU_7	Operational support to Primary Data Storage solutions	Must have
The Surveillance Data Storage provider shall provide the different Primary Data Storage providers with the necessary operational support (e.g. credentials, configuration information, documentation, sample data, connectivity verification, issues monitoring, test sets, etc.) to facilitate a smooth production functioning of the solutions involved.		

System Qualities – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
Source: Contractor's expertise		
RQ_TTSU_SU_8	Support to connectivity tests with ID Issuer solutions	Must have
The Surveillance Data Storage provider shall provide the ID Issuer solution providers with the necessary support (e.g. credentials, configuration information, documentation, sample data, test sets, etc.) to verify the compliance of their client implementations prior to the connection to production.		
Source: Contractor's expertise		
RQ_TTSU_SU_9	Operational support to ID Issuer solutions	Must have
The Surveillance Data Storage provider shall provide the ID Issuer solution providers with the necessary operational support (e.g. credentials, configuration information, documentation, sample data, connectivity verification, issues monitoring, test sets, etc.) to facilitate a smooth production functioning of the solutions involved.		
Source: Contractor's expertise		
RQ_TTSU_SU_10	Support to interface versioning	Must have
The Surveillance Data Storage provider shall support any data model or functionality evolution through the release of a new interface version compliant with the new features.		
Source: Contractor's expertise		

3.8.1.2.2. Security

Security – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
RQ_TTSU_SE_1	Data isolation	Must have
The Surveillance Data Storage provider shall provide economic operators with a secure and segmented hosting environment with server, storage, and network elements that are logically isolated from other economic operators running on the same infrastructure.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
Source: Contractor's expertise		
RQ_TTSU_SE_2	User access authorisation	Must have
The Surveillance Data Storage shall provide a user authorisation mechanism in order to ensure the segregation of responsibilities and restrict access to data.		
Source: Article 15(7) and 15(9) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_SE_3	Auditability	Must have
The Surveillance Data Storage shall provide auditing, an audit trail with change recording, and an activity logging mechanism with timestamps for all data-related activities.		
Source: Article 15(8) (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_SE_4	Audit logging	Must have

Security – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
<p>The Surveillance Data Storage shall record important events together with the user who performs the operation in an audit log, which shall be centrally maintained. The list of events the Surveillance Data Storage shall record in the audit log shall include but not be limited to the following:</p> <ul style="list-style-type: none"> • Database activities • Technical events, like data synchronisation and data replication • Accessing of data 		
Source: Contractor's expertise		
RQ_TTSU_SE_5	Error logging	Must have
All errors and faults in the system shall be recorded in an error log, which shall be centrally maintained.		
Source: Contractor's expertise		
RQ_TTSU_SE_6	Completeness of logs	Must have
<p>The error log and audit log shall contain all required information in order to provide the authorised user with interpretable and comprehensive information about the cause of the error, audit traceability for the actions taken by an authorised user.</p>		
Source: Contractor's expertise		
RQ_TTSU_SE_7	Auditing and monitoring plan	Must have
<p>The Surveillance Data Storage provider shall implement an auditing and monitoring plan. The plan shall address, but not be limited to, the following topics:</p> <ul style="list-style-type: none"> • Auditing of vulnerabilities and threats • Auditing of data access • Auditing of database baseline • Monitoring of suspicious activities • Monitoring of systems health • Anomalies detection • Implement server hardening guidelines for securing the system 		
Source: Use case – Auditing of Data Storage		
RQ_TTSU_SE_8	End-to-end traceability	Must have
<p>The Surveillance Data Storage shall ensure that any data/action can always be traced to its original source (i.e. economic operator facility or ID Issuer).</p>		
Source: Contractor's expertise		
RQ_TTSU_SE_9	Auditor support	Must have
<p>The Surveillance Data Storage provider shall provide full access and any requested evidence to the independent external auditor to ensure that s/he can monitor the activities of the Surveillance Data Storage provider and the accesses to the system.</p>		
Source: Article 15(8) (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_SE_10	Log preservation	Must have
<p>The Surveillance Data Storage shall archive the error and audit logs, using integrity checking countermeasures to ensure that the log file has been archived successfully after each archiving process.</p>		
Source: Contractor's expertise		

Security – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
RQ_TTSU_SE_11	Log retention period	Must have
Access logs shall be immutable and kept for at least four (4) years. Error logs shall be immutable and kept for at least two (2) years.		
Source: Contractor's expertise		
RQ_TTSU_SE_12	Sender tracking	Must have
The Surveillance Data Storage shall resolve and authenticate the sender's identity against a trusted identity provider. Messages sent from an unauthenticated sender shall not be accepted.		
Source: Contractor's expertise		
RQ_TTSU_SE_13	Checksum verification	Must have
The Surveillance Data Storage shall verify the message checksum to ensure that the data was not tampered with. Messages where the checksum is not valid shall not be accepted.		
Source: Contractor's expertise		
RQ_TTSU_SE_14	Secure coding practice	Must have
The Surveillance Data Storage provider shall provide a system implementation compliant with common secure coding practices such as OWASP.		
Source: Contractor's expertise		
RQ_TTSU_SE_15	User access authentication	Must have
The Surveillance Data Storage shall provide a user authentication mechanism prior to any access to system resources and data.		
Source: Contractor's expertise		
RQ_TTSU_SE_16	Password strength	Must have
The Surveillance Data Storage shall ensure the enforcement of password standards (e.g. minimum length and use of alpha, numeric and special characters.) and, when applicable, establish a specified period for password expiration and prohibit the user from reusing recent passwords.		
Source: Contractor's expertise		
RQ_TTSU_SE_17	Password protection	Must have
The Surveillance Data Storage shall ensure that user passwords are non-printing and non-displaying.		
Source: Contractor's expertise		
RQ_TTSU_SE_18	Integration with the European single sign-on mechanism	Should have
The Surveillance Data Storage should provide integration with the European access control mechanism (i.e. "EU Login") to allow, when applicable, competent authorities to use single sign-on to the system.		
Source: Contractor's expertise		

3.8.1.2.3. Data protection

Data Protection – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
RQ_TTSU_DP_1	Data protection rules	Must have
The Surveillance Data Storage provider shall be compliant with and ensure that personal data is processed and protected in accordance with EU Regulation 2016/679 (European Commission - REGULATION (EU) 2016/679, 2016), which repeals Directive 95/46/EC.		
Source: Article 15(10) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_DP_2	Antitrust	Must have
The data confidentiality must follow all the necessary safeguarding measures respecting the current ruling of antitrust, in order to prevent leak or access of any sensitive data of an economic operator by any other economic operator.		
Source: Contractor's expertise		
RQ_TTSU_DP_3	Confidentiality treatment	Must have
The Surveillance Data Storage provider must treat with confidentiality any information or documents disclosed, in any format exchanged or stored in the system.		
Source: Contractor's expertise		

3.8.1.2.4. System constraints

System Constraints – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
RQ_TTSU_SC_1	Facility location	Must have
The Surveillance Data Storage facility shall be physically located within the territory of the European Union, and any maintenance on the servers shall be carried out within the European Union.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTSU_SC_2	Extension of guarantees	Must have
Any additional exchange of data and metadata that might occur in the Surveillance Data Storage facility with the objective to implement or support the Tracking and Tracing System shall be guaranteed the same level of data protection and quality defined for the rest of the system.		
Source: Contractor's expertise		
RQ_TTSU_SC_3	Non-limiting throughput for economic operators	Must have
The overall throughput of the Surveillance Data Storage shall not be a limiting factor for the speed of the manufacturing production lines or for the logistics activities of the importers, distributors or wholesalers.		
Source: Contractor's expertise		
RQ_TTSU_SC_4	Data dictionary compatibility	Must have
The Surveillance Data Storage shall ensure that the physical storage of the Tracking and Tracing data conforms to the data dictionary described in section 3.11.		
Source: Contractor's expertise		
RQ_TTSU_SC_5	Data validation rules	Must have

System Constraints – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
The Surveillance Data Storage solution shall implement Tracking and Tracing data validation rules conformant with the common validation rules described in section 3.12.		
Source: Contractor's expertise		
RQ_TTSU_SC_6	Messaging compatibility	Must have
The Surveillance Data Storage solution shall exchange messages conformant with the specifications described in section 3.5.1.		
Source: Contractor's expertise		
RQ_TTSU_SC_7	Decoupling of operations	Must have
The Surveillance Data Storage must decouple data acquisition from data processing, avoiding unnecessary coupling between independent processes.		
Source: Contractor's expertise		
RQ_TTSU_SC_8	Event-driven design	Must have
The Surveillance Data Storage shall be designed based on an event-driven architectural pattern for the data acquisition and data processing components.		
Source: Contractor's expertise		
RQ_TTSU_SC_9	Fault isolation	Must have
The main components of the Surveillance Data Storage shall be designed to support fault isolation, in order not to propagate its errors to other components of the solution and limit the impact of any problem to the minimum.		
Source: Contractor's expertise		
RQ_TTSU_SC_10	Designed for monitoring	Must have
The Surveillance Data Storage solution shall be designed for monitoring in order to help the provider in the identification of current, potential or future issues (e.g. performance, code bugs, application errors, security threats, etc.). The monitoring should be applied at the following levels: hardware, software, infrastructure and application (the latter aiming at reporting on "what is the problem").		
Source: Contractor's expertise		
RQ_TTSU_SC_11	Idempotent messages	Must have
The Surveillance Data Storage message management shall be designed to avoid acquiring and reprocessing the same message multiple times, since messages of the Tracking and Tracing System are not idempotent.		
Source: Contractor's expertise		
RQ_TTSU_SC_12	Usage of an agnostic query language to retrieve the canonical data model	Should have
The Surveillance Data Storage should provide an interface compliant with some agnostic query language to retrieve data from the Tracking and Tracing canonical data model. As such, the Resource Query Language (RQL), which is an open language (apsstandard - RQL, 2014) for querying collections of resources, could be a potential solution.		
Source: Contractor's expertise		

3.8.1.2.5. System interfaces

Interface SU2DW	
ID	Name
▪ SU2DW	▪ Surveillance Data Storage to distributors and wholesalers
Owner System	
▪ Surveillance Data Storage solution	
Data Source	Data Target
▪ Component established at the facilities of the distributors or wholesalers to report events	▪ Surveillance Data Storage
Data Type	
<ul style="list-style-type: none"> ▪ Operational event messages ▪ Transactional event messages 	
Interface Trigger	
▪ Push upon request by the client systems of the economic operators.	
Access Control	
▪ Only authorised wholesalers and distributors have access to this interface.	
Description	
▪ This interface provides the event information reporting channel for wholesalers and distributors.	

Interface SU2CA	
ID	Name
▪ SU2CA	▪ Surveillance Data Storage to competent authorities
Owner System	
▪ Surveillance Data Storage solution	
Data Source	Data Target
▪ Surveillance Data Storage	▪ Competent authorities
Data Type	
<ul style="list-style-type: none"> ▪ Operational event messages ▪ Transactional event messages ▪ Data extraction messages ▪ Lookup tables ▪ Notifications 	
Interface Trigger	
<ul style="list-style-type: none"> ▪ Pull execution on demand ▪ Push execution on demand ▪ Push scheduled execution 	
Access Control	
▪ Only the competent authorities have access to this interface.	
Description	
▪ This interface provides the channel to give competent authorities full access to the Surveillance Data Storage.	

Interface SU2AU	
ID	Name
▪ SU2AU	▪ Surveillance Data Storage to auditors
Owner System	
▪ Surveillance Data Storage solution	

Data Source	Data Target
▪ Surveillance Data Storage	▪ Auditors
Data Type	
<ul style="list-style-type: none"> ▪ Operational event messages ▪ Transactional event messages ▪ Data extraction messages ▪ Lookup tables ▪ Notifications 	
Interface Trigger	
▪ Pull execution on demand	
Access Control	
▪ Only the auditors have access to this interface.	
Description	
▪ This interface provides the channel to give auditors access to the auditing data of the Surveillance Data Storage.	

Interface SU2PR	
ID	Name
▪ SU2PR	▪ Surveillance Data Storage to Primary Data Storage
Owner System	
▪ Surveillance Data Storage solution	
Data Source	Data Target
▪ Primary Data Storage	▪ Surveillance Data Storage
Data Type	
<ul style="list-style-type: none"> ▪ Operational event messages ▪ Transactional event messages 	
Interface Trigger	
<ul style="list-style-type: none"> ▪ Push execution on demand ▪ Push scheduled execution 	
Access Control	
▪ Only the Primary Data Storage has access to this interface.	
Description	
▪ This interface provides the channel to update the Surveillance Data Storage with Primary Data Storage data.	

Interface SU2II	
ID	Name
▪ SU2II	▪ Surveillance Data Storage to ID issuer
Owner System	
▪ Surveillance Data Storage solution	
Data Source	Data Target
▪ ID issuer	▪ Surveillance Data Storage
Data Type	
▪ Issuance of serial numbers messages	
Interface Trigger	
▪ Push execution on demand	
Access Control	

<ul style="list-style-type: none"> Only the ID Issuers have access to this interface.
Description
<ul style="list-style-type: none"> This interface provides the channel to ID Issuers to report the issuance of serial numbers

3.8.1.3. Applicable standards

Applicable Standards – Tracking and Tracing System – Surveillance Data Storage		
ID	Name	Priority
RQ_TTSU_AS_1	ISO 27001 compliant hosting	Must have
The Surveillance Data Storage shall be hosted in an ISO 27001 compliant hosting. This provider is expected to deliver a highly available, scalable, and flexible data storage platform.		
Source: Contractor's expertise		
RQ_TTSU_AS_2	Character set content	Must have
The Surveillance Data Storage shall store content using the ISO/IEC 8859-15:1999 character set.		
Source: Contractor's expertise		

3.9. Repository Router

The Repository Router is a component of the Surveillance Data Storage solution, which is specifically designed to handle massive amounts of data ingestion. The distributors and wholesalers push data events to the Repository Router, where the data can take multiple paths depending on the manufacturer/importer of the items referred to in the event. The Router acts as a high-performance data ingestion layer dealing with a massive amount of data events.

The Primary Data Storages of the different manufacturers/importers receive the events that are relevant for them from the Repository Router.

Below, the requirements of the Repository Router component are specified.

3.9.1. Requirements specification

3.9.1.1. Functional

Functional Requirements – Tracking and Tracing System – Repository Router		
ID	Name	Priority
RQ_TTRR_FU_1	Event acquisition	Must have
The Repository Router shall provide one endpoint through which distributors, wholesalers or ID Issuers deliver one or more messages at a time.		
Source: Contractor's expertise		
RQ_TTRR_FU_2	Event recording	Must have
The Repository Router shall ensure that all events are validated and recorded in the Surveillance Data Storage.		
Source: Contractor's expertise		
RQ_TTRR_FU_3	Submission to interested parties	Must have

Functional Requirements – Tracking and Tracing System – Repository Router		
ID	Name	Priority
The Repository Router shall ensure that all events received from distributors and wholesalers are submitted to the Primary Data Storage of the manufacturer/importer of the items referred to in the event.		
Source: Contractor's expertise		
RQ_TTRR_FU_4	Storage of orphan events	Must have
The Repository Router shall store orphan events for which the manufacturer/importer of the items referred to in the event is unknown, until this information becomes available and the event is submitted to a Primary Data Storage.		
Source: Contractor's expertise		

3.9.1.2. Technical

3.9.1.2.1. System qualities

System Qualities – Tracking and Tracing System – Repository Router		
ID	Name	Priority
RQ_TTRR_RE_1	Message replay-ability	Must have
The Repository Router shall persist the outgoing messages until the messages are successfully delivered. When trying to transmit the outgoing messages, the Repository Router shall handle transient failures by transparently retrying a failed operation. A durable queue could be a cost-effective implementation alternative.		
Source: Contractor's expertise		
RQ_TTRR_RE_2	Data reception acknowledgment	Must have
The Repository Router shall return an acknowledgement of a successful data receipt to the sender, otherwise failing with a consistent error code.		
Source: Contractor's expertise		
RQ_TTRR_RE_3	High availability	Must have
The Repository Router shall be available for use with an uptime target of 99.55% (Tier III data centre).		
Source: Contractor's expertise		
RQ_TTRR_PE_1	Messaging throughput	Must have
The Repository Router shall support rates of message throughput for input/output operations in the range of 750 thousand (750,000) messages per second per instance.		
Source: Contractor's expertise		
RQ_TTRR_PE_2	Minimum concurrency level	Must have
The Repository Router shall support one thousand (1,000 simultaneously connected clients).		
Source: Contractor's expertise		
RQ_TTRR_PE_3	Minimum scalability	Must have
The Repository Router shall support traffic spikes up to an average of 20% higher than normal demand.		

System Qualities – Tracking and Tracing System – Repository Router		
ID	Name	Priority
Source: Contractor's expertise		

3.9.1.2.2. Security

Security – Tracking and Tracing System – Repository Router		
ID	Name	Priority
RQ_TTRR_SE_1	Sender tracking	Must have
The Repository Router shall resolve and authenticate the sender's identity against a trusted identity provider. Messages sent from an unauthenticated sender shall not be accepted.		
Source: (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTRR_SE_2	Checksum verification	Must have
The Repository Router shall verify the message checksum to ensure that the data was not tampered with. Messages where the checksum is not valid shall not be accepted.		
Source: (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		

3.9.1.2.3. System constraints

System Constraints – Tracking and Tracing System – Repository Router		
ID	Name	Priority
RQ_TTRR_SC_1	Messaging compatibility	Must have
The Repository Router shall exchange messages conformant with the specification described in section 3.5.1.		
Source: Contractor's expertise		
RQ_TTRR_SC_2	Decoupling of operations	Must have
The Repository Router must decouple the data acquisition from data processing, avoiding unnecessary coupling between independent processes.		
Source: Contractor's expertise		
RQ_TTRR_SC_3	Event-driven design	Must have
The Repository Router shall be designed based on an event-driven architectural pattern for the data acquisition and data processing components.		
Source: Contractor's expertise		
RQ_TTRR_SC_4	Fault isolation	Must have
The main components of the Repository Router shall be designed to support fault isolation, in order not to propagate its errors to other components of the solution and limit the impact of any problem to the minimum.		
Source: Contractor's expertise		
RQ_TTRR_SC_5	Idempotent messages	Must have

System Constraints – Tracking and Tracing System – Repository Router		
ID	Name	Priority
The Repository Router message management shall be designed to avoid acquiring and reprocessing the same message multiple times, since messages of the Tracking and Tracing System are not idempotent.		
Source: Contractor’s expertise		

3.10. System for the issuance of unique identifiers

The Tracking and Tracing System comprises an **ID Issuer solution** that generates the codes necessary to assure the uniqueness of the unique identifier. The responsibilities of the ID Issuer solution are threefold:

- a. provision of codes to the economic operators for their activities;
- b. notification to the central Surveillance Data Storage solution of which codes have been provisioned (later, the Repository Router of the Surveillance will transmit these codes to the proper Primary Data Storage); and
- c. registration services to the economic operators, which allow the population of lookup data needed for the unique identifier serialisation.

The lookup registers are related to economic operators, facility of manufacturing, and machine of manufacturing. The codes are related either to unit packets of tobacco products or to aggregation packaging levels.

The ID Issuer solution shall be established by an independent third party code provider, which will be responsible for generating codes according to certain rules (e.g. prescribed format, uniqueness, minimum guess probability, not predictable, etc.). On this regard, It is envisaged that the System will comprise one ID Issuer solution, appointed by each Member State.

It is advised that the selection of the ID Issuer is done by the competent authorities in each of the 28 EU Member States, ensuring that this critical process – the generation of the serial numbers – is always under their control. Each Member State shall select an ID Issuer, or some of them could create clusters to contract jointly an ID Issuer, for the sake of efficiency and economies of scale. This may result on the selection of up to 28 ID Issuers.

To avoid the risk of generating duplicate codes, unique prefixes shall be allocated to each of the ID Issuers, to be incorporated in the codes generated. This practice is endorsed by (ISO/IEC 15459:2014 - Unique identification, 2014).

Below, the requirements of the ID Issuer solution are specified.

3.10.1. Requirements specification

3.10.1.1. Functional

Functional Requirements – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority

Functional Requirements – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
RQ_TTII_FU_1	Generation of codes	Must have
<p>The ID Issuer solution shall generate codes, which ensure the uniqueness of the unique identifier, at the request of economic operators that have been authorised previously.</p> <p>For the unit level, ID Issuers shall be responsible for the generation of a code consisting of the elements:</p> <ul style="list-style-type: none"> • The alphanumeric characters that constitute the ID issuer identification code assigned. • An alphanumeric sequence ('serial number'); • A code ('product code') allowing for the determination of the following: <ul style="list-style-type: none"> ○ the place of manufacturing; ○ the manufacturing facility referred to in Article 16; ○ the machine used to manufacture the tobacco products referred to in Article 18; ○ the product description; ○ the intended market of retail sale; ○ the intended shipment route; ○ where applicable, the importer into the Union; <p>For the aggregated level, ID Issuers shall be responsible for the generation of a code consisting of the elements:</p> <ul style="list-style-type: none"> • The alphanumeric characters that constitute the ID issuer identification code assigned . • An alphanumeric sequence ('serial number'); • The identifier code of the facility in which the aggregation process took place. 		
Source: Article 15(6) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTII_FU_2	Generation rules of serial numbers	Must have
<p>The generation of serial numbers shall follow the rules below:</p> <ul style="list-style-type: none"> • Serial numbers are generated on a demand-driven basis. • Production needs shall not be predictable through the serial number. • The allocation of sequential numbers per economic operator shall be avoided. • The allocation of predefined ranges of serial numbers per economic operator shall be avoided. • The ID Issuer solution uses a collection of data (i.e. primary information), which has been provided by the economic operator, to generate a serial number. • Each serial number shall be random. • The probability of guessing a serial number is negligible. • The serial number generated shall include some security features to facilitate the authentication of the product. • The ID Issuer solution shall avoid duplications of serial numbers for a specific combination of primary information. 		
Source: Section 2.1.4		
RQ_TTII_FU_3	Registration of lookup data	Must have
<p>The ID Issuer solution shall allow that the economic operators register the following lookup information, namely: economic operator, facility of manufacturing, and machine of manufacturing.</p>		
Source: Contractor's expertise		
RQ_TTII_FU_4	Recall of messages	Must have
<p>The ID Issuer solution shall accept the recall of messages in such a way that any code generation request, within 24h after the arrival of that request, can be recalled. Therefore, ID Issuer solutions shall wait 24h before stating processing the generation of codes.</p>		
Source: Contractor's expertise		
RQ_TTII_FU_5	Stored data - prevent economic operator's access	Must have

Functional Requirements – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
The ID Issuer solution shall prevent that any economic operator involved in the trade of tobacco products can update or delete any data stored in its storage.		
Source: Article 15(9) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTII_FU_6	Codes – notification	Must have
Once the ID Issuer solution has successfully generated codes, they shall be transmitted to the Surveillance Data Storage. Later, the Repository Router of the Surveillance will transmit these codes to the proper Primary Data Storage.		
Source: Article 15(6) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTII_FU_7	Data access authorization	Must have
The ID Issuer solution shall provide and limit data access only to authorized users.		
Source: Article 15(8) and 15(9) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTII_FU_8	Logic data deletion	Must have
Tracking and Tracing data records may be only logically deleted until the moment of the definitive data purge, according with the required data retention period.		
Source: Contractor's expertise		
RQ_TTII_FU_9	Data retention period	Must have
The ID Issuer solution shall provide a retention period of at least 10 years after the generation of the codes. Records related to codes must be kept accessible during this period.		
Source: (everis, 2017)		
RQ_TTII_FU_10	Operations audit trail	Must have
The ID Issuer solution shall provide and keep audit trails (log) for every data access related to the Tracking and Tracing System. Every data change must be logged including the original value. The audit trail shall contain at least the following information:		
<ul style="list-style-type: none"> • Audit ID: A unique unchangeable auto-number containing the audit key • Edit Date: A Date/Time containing the timestamp of the change • User: The user ID who made the change • Record ID: The value that uniquely identifies the changed record • Source: The name of the object (table/view/document) that contains the changed record • Field: The name of the changed field • Before Value: The value before the change 		
Source: Contractor's expertise		
RQ_TTII_FU_11	Economic operator approval	Must have
The economic operators that require access to the ID Issuer solution shall be approved (i.e. authorised) previously in order to avoid that illicit trade entities access to valid codes.		
Source: Contractor's expertise		
RQ_TTII_FU_12	User authentication and authorisation	Must have

Functional Requirements – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
The ID Issuer solution shall establish an authentication and authorisation mechanism prior any system access.		
Source: Contractor's expertise		
RQ_TTII_FU_13	Change the user password	Must have
The ID Issuer solution provider shall establish a mechanism to allow the user to change its own password.		
Source: Contractor's expertise		
RQ_TTII_FU_14	Recover the user password	Must have
The ID Issuer solution provider shall establish a mechanism to allow the user to recover its own password.		
Source: Contractor's expertise		
RQ_TTII_FU_15	Deactivate user	Must have
The ID Issuer solution provider shall establish a mechanism to allow System Administrators to deactivate a user, where necessary.		
Source: Contractor's expertise		
RQ_TTII_FU_16	Re-activate user	Must have
The ID Issuer solution provider shall establish a mechanism to allow System Administrators to re-activate a user.		
Source: Contractor's expertise		

3.10.1.2. Technical

3.10.1.2.1. System qualities

System Qualities – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
RQ_TTII_RE_1	Data Reception Acknowledgment	Must have
The ID Issuer solution shall acknowledge the sender regarding a successful data receipt, otherwise failing with a consistent error code.		
Source: Contractor's expertise		
RQ_TTII_RE_2	Business Continuity & Disaster Recovery	Must have
The ID Issuer solution provider shall provide data resilience and disaster recovery capabilities across multiple sites.		
Source: Contractors' expertise		
RQ_TTII_RE_3	Data Backups	Must have
The ID Issuer solution provider shall take periodic full and/or incremental snapshots of the data store to mitigate the risk of system/storage failure.		

System Qualities – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTII_RE_4	Outbound Channel Redundancy	Must have
The ID Issuer solution shall be able to change automatically to additional outbound communication channels (at least one shall be established) in case the message submission fails due to a communication error with the Surveillance Data Storage.		
Source: Contractor's expertise		
RQ_TTII_PE_1	Storage Size	Must have
The ID Issuer solution shall be able to support storage size for the codes of at least 5 Terabytes per instance yearly.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014), (everis, 2017)		
RQ_TTII_PE_2	Messaging Throughput	Must have
The ID Issuer solution shall support rates of message throughput for input/output operations in the range of one thousand messages per second per instance.		
Source: (everis, 2017)		
RQ_TTII_PE_3	Query Request Throughput	Must have
The ID Issuer solution shall be able to support at least 10 concurrent query requests per instance.		
Source: (everis, 2017)		
RQ_TTII_PE_4	Network Uptime	Must have
The ID Issuer solution facility shall be able to meet the Network Uptime Target: 99.99%.		
Source: Contractor's expertise		
RQ_TTII_PE_5	Server Uptime	Must have
The ID Issuer solution facility shall be able to meet the Server Uptime Target: 99.99%.		
Source: Contractor's expertise		
RQ_TTII_PE_6	Latency intra data centre	Must have
The ID Issuer solution facility shall be able to meet the Latency Target: Less than 100 millisecond latency between physical servers in the same data centre.		
Source: Contractor's expertise		
RQ_TTII_PE_7	Inter data centre speed	Must have
The ID Issuer solution facility shall be able to meet the Speed Target: at least 100 Mbps between the different data centres involved, namely: Surveillance Data Storage solution and Primary Data Storage solutions.		
Source: Contractor's expertise		
RQ_TTII_PE_8	Support Response Time SMO	Must have

System Qualities – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
The ID Issuer solution provider shall be able to meet the Support Response Time Target – 30 minute Support Response Time Target for Emergency Incidents.		
Source: Contractor’s expertise		
RQ_TTII_PE_9	Hardware Break/Fix SMO	Must have
The ID Issuer solution provider shall be able to meet the Hardware Break/Fix Target – Subject to the vendor-backed support.		
Source: Contractor’s expertise		
RQ_TTII_PE_10	Data Archiving	Must have
The ID Issuer solution provider shall archive data that is no longer required for use from the system, being compliant with the maximum retention period required, thus reducing the size of the data store.		
Source: Contractor’s expertise		
RQ_TTII_PE_11	Data Centre Efficiency	Should have
The ID Issuer solution provider should be compliant with the European Code of Conduct for Energy Efficiency in Data Centres, and use of best practices for data centre energy efficiency.		
Source: (European Commission - JRC, 2017)		
RQ_TTII_SU_1	Scalability	Must have
The ID Issuer solution facility shall be scalable and technically upgradeable to maintain performance against threat growth. This includes I/O performance, storage, and network capacity and licences.		
Source: Contractor’s expertise		
RQ_TTII_SU_2	Unlimited by Design	Must have
The ID Issuer solution shall have growth potential beyond the figures given in this section to indicate processing capacity, or storage capacity, and shall not deem any limitation on design.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTII_SU_3	Support to connectivity tests with economic operator	Must have
The ID Issuer solution provider shall provide to the economic operator(s), which have been authorised to use this generation solution, the necessary support (e.g. credentials, configuration information, documentation, sample data, test sets, etc.) to verify the compliance of their client implementations prior the connection to production.		
Source: Contractor’s expertise		
RQ_TTII_SU_4	Operational support to economic operator	Must have
The ID Issuer solution provider shall provide to the economic operator(s), which have been authorised to use this generation solution, the necessary operational support (e.g. credentials, configuration information, documentation, sample data, connectivity verification, issues monitoring, test sets, etc.) to facilitate a smooth production functioning of their client implementations.		
Source: Contractor’s expertise		
RQ_TTII_SU_5	Support to interface versioning	Must have

System Qualities – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
The ID Issuer solution provider shall support any data model or functionality evolution through the release of a new interface version compliant with the new features.		
Source: Contractor's expertise		

3.10.1.2.2. Security

Security – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
RQ_TTII_SE_1	Data isolation	Must have
The ID Issuer solution provider shall provide economic operators with a secure and segmented hosting environment with server, storage, and network elements that are logically isolated from other economic operators running on the same infrastructure.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTII_SE_2	Data protection	Must have
The ID Issuer solution shall use a tamper-proof method to record the data that preserve the records in a non-rewritable, non-erasable form.		
Source: Contractor's expertise		
RQ_TTII_SE_3	User access authorisation	Must have
The ID Issuer solution shall provide a user authorisation mechanism in order to ensure the segregation of responsibilities and to restrict access to data.		
Source: Article 15(7) and 15(9) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTII_SE_4	Auditability	Must have
The ID Issuer solution shall provide auditing, audit trail with change recording, and activity logging mechanism with timestamps for all data-related activities.		
Source: Article 15(8) (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTII_SE_5	Audit logging	Must have
The ID Issuer solution shall record important events together with the user who performs the operation into an audit log, which shall be centrally maintained. The list of events the ID Issuer solution shall record in the audit record shall include but not be limited to the following: <ul style="list-style-type: none"> • Database activities • Technical events like data synchronisation and data replication • Accessing of data 		
Source: Contractor's expertise		
RQ_TTII_SE_6	Error logging	Must have
All errors and faults in the ID Issuer solution shall be recorded in an error log, which shall be centrally maintained.		
Source: Contractor's expertise		

Security – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
RQ_TTII_SE_7	Completeness of logs	Must have
The error log and audit log shall contain all required information in order to provide the authorised user with interpretable and comprehensive information about the cause of the error, as well as the audit traceability for the actions authorised for a user.		
Source: Contractor's expertise		
RQ_TTII_SE_8	End-to-end traceability	Must have
The ID Issuer solution shall ensure that any data/action can always be traced to its original source (i.e. client application of manufacturer/importer/distributor/wholesaler).		
Source: Contractor's expertise		
RQ_TTII_SE_9	Auditor support	Must have
The ID Issuer solution provider shall provide full access and any requested evidence to the independent external auditor to ensure that he can monitor the activities of the provider and the accesses to the solution.		
Source: Article 15(8) (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTII_SE_10	Log preservation	Must have
The ID Issuer solution shall archive the error and the audit log, using integrity checking countermeasures to ensure that the log file has been archived successfully after each archiving process.		
Source: Contractor's expertise		
RQ_TTII_SE_11	Log retention period	Must have
Access logs shall be immutable and kept for at least 4 years. Error logs shall be immutable and kept for at least 2 years.		
Source: Contractor's expertise		
RQ_TTII_SE_12	Sender Tracking	Must have
The ID Issuer solution shall resolve and authenticate the sender's identity against a trusted identity provider. Messages sent from an unauthenticated sender shall not be accepted.		
Source: Contractor's expertise		
RQ_TTII_SE_13	Checksum Verification	Must have
The ID Issuer solution shall verify the message checksum to ensure that the data was not tampered with. Messages where the checksum is not valid shall not be accepted.		
Source: Contractor's expertise		
RQ_TTII_SE_14	User access authentication	Must have
The ID Issuer solution shall provide a user authentication mechanism prior any access to system resources and data.		

Security – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
Source: Contractor's expertise		
RQ_TTII_SE_15	Password strength	Must have
The ID Issuer solution shall ensure the enforcement of password standards (e.g., minimum length and use of alpha, numeric and special characters.) and when applicable, with the establishment of a specified period for password expiration and accommodate prohibiting the user from reusing recent passwords.		
Source: Contractor's expertise		
RQ_TTII_SE_16	Password protection	Must have
The ID Issuer solution shall ensure that user passwords are non-printing and non-displaying.		
Source: Contractor's expertise		

3.10.1.2.3. Data protection

Data Protection – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
RQ_TTII_DP_1	Data protection rules	Must have
The ID Issuer solution provider shall be compliant with the current European data protection regulation to ensure that personal data is processed and protected in accordance with the rules and safeguards laid down in EU Regulation 2016/679 (European Commission - REGULATION (EU) 2016/679, 2016), which repeals Directive 95/46/EC.		
Source: Article 15(10) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		

3.10.1.2.4. System constraints

System Constraints – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
RQ_TTII_SC_1	Code number format	Must have
The serial number shall be a numeric or alphanumeric sequence of maximum 20 characters.		
Source: Contractor's expertise		
RQ_TTII_SC_2	Probability of code guessing	Must have
The probability that the code can be guessed shall be negligible and in any case lower than one in ten thousand. For that purpose, the number generation could rely on randomisation techniques.		
Source: Article 4(c) of (Commission Delegated Regulation (EU) 2016/161 - FMD, 2015)		
RQ_TTII_SC_3	Facility location	Must have

System Constraints – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
The ID Issuer solution facility shall be physically located on the territory of the European Union, and any maintenance on the servers shall be carried out within the European Union.		
Source: Article 15(8) of (Directive 2014/40/EU of the European Parliament and of the Council, 2014)		
RQ_TTII_SC_4	Extension of guarantees	Must have
Any additional exchange of data and metadata that might occur in the ID Issuer solution facility with the objective to implement or support the Tracking and Tracing System shall be guaranteed the same level of data protection and quality defined for the rest of the system.		
Source: Contractor's expertise		
RQ_TTII_SC_5	Not limiting throughput for economic operators	Must have
The overall throughput of the ID Issuer solution shall not be a limiting factor for the speed of the manufacturing production lines or for the importer, distributor and wholesaler logistics activities.		
Source: Contractor's expertise		

3.10.1.2.5. System interfaces

Interface II2EO	
ID	Name
▪ II2EO	▪ ID Issuer to economic operators
Owner System	
▪ ID Issuer solution	
Data Source	Data Target
▪ ID Issuer solution	▪ Economic operator
Data Type	
▪ Registration messages ▪ Code issuance messages	
Interface Trigger	
▪ Push upon request by the client systems of the economic operators.	
Access Control	
▪ Only authorized economic operators have access to this interface.	
Description	
▪ This interface provides the code generation channel to the economic operators.	

3.10.1.3. Applicable standards

Applicable Standards – Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
RQ_TTII_AS_1	Unique prefix - ISO/IEC 15459:2014	Must have

Applicable Standards –Tracking and Tracing System – ID Issuer solution		
ID	Name	Priority
To avoid the risk of generating duplicate codes, unique prefixes shall be allocated to each of the ID Issuers, to be incorporated in the codes generated. This practice is endorsed by (ISO/IEC 15459:2014 - Unique identification, 2014).		
Source: Contractors' expertise		

3.11. Data Dictionary

This section sets out a recommended outline for a data dictionary, which should be developed by the provider of Surveillance Data Storage.

3.11.1. Registered entities

The economic operators have to register into the System information that is only known by them, namely: economic operator details, facilities for manufacturing, and machines within these facilities. This data is represented in the data dictionary as part of the following entities:

- EconomicOperator
- Facility
- ManufacturingMachine

The economic operators are responsible for registering, through the appropriate ID Issuer solution, the information related to these entities. The ID Issuer solution will populate the new information into the entities when a valid request for registration/correction/de-registration is successfully processed (see details of messaging in 3.5.2). It should be noted that a de-registration request only implies a change on the register status, not a physical deletion of the information. Once the entity data is populated within the ID Issuer solution, this register is replicated to the Surveillance Data Storage, which will route it to the Primary Data Storage solutions that may require it to ensure referential integrity.

3.11.2. Lookup entities to support the decoding of the unique identifier elements

The data dictionary also includes some lookup entities that host the necessary information that facilitates the readability of the codes that compose the unique identifier. The lookup entities are as follow:

- ProductDescription
- ManufacturingActivitiesLocation
- Importer
- ShipmentRouteAndMarket

On one hand, the ProductDescription entity is populated by the Primary Data Storage, which processes the notification of codes issuance at unit packet level.

On the other hand, the ManufacturingActivitiesLocation entity is populated with the information provided by the economic operators in the registration process of the following entities: EconomicOperator, Facility and ManufacturingMachine. When the information is consolidated within the ID Issuer solution, the registers have to be replicated to the Surveillance Data Storage, which consolidates the appropriate fields into the entity.

Finally, the UnitPacketLevelDate, AggregationPackagingLevelDate and ShipmentRouteAndMarket entities are pre-loaded by the solution provider since the potential combinations can be known in advance. Concerning UnitPacketLevelDate, it is responsible for encoding in an optimised way and according the rules detailed in 2.1.1.4, namely: the date of the manufacturing activities up to the day (e.g. 2016-02-24). Regarding the AggregationPackagingLevelDate, it is also responsible for encoding the date of the manufacturing activities according to the rules detailed in 2.2.1.3, but up to the month (e.g. 2016-02). The ShipmentRouteAndMarket shall be pre-loaded according the rules detailed in 2.1.1.4. All potential values of the dates shall be pre-loaded by the provider in the appropriate table.

The Surveillance Data Storage acts as the common data repository where the competent authorities shall synchronise the lookup data, which is necessary to decode the elements of the unique identifiers, into their client hand-held devices.

3.11.3. Canonical data model

Finally, on the basis of the data dictionary entities introduced above, the canonical data model has been derived as follows:

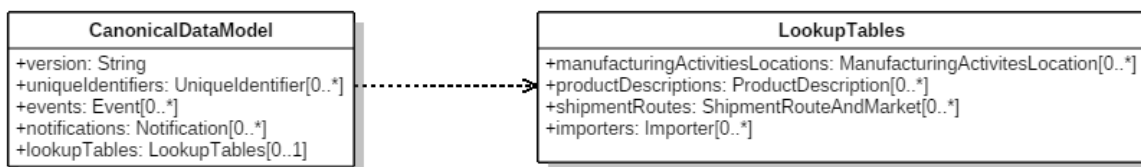


Figure 11: Canonical data model entity diagram

As can be noticed, the **canonical data model supports versioning** in order to facilitate the integration of future changes to the canonical data model. Thus, the consumer applications may be adapted according the versioning information, and the storage providers must support different canonical data model versions until a major incompatibility arises.

The canonical data model is an independent and abstract protocol that, for integration purposes with multiple parties and multiple scenarios, could be mapped to different open standard data protocols such as XML (W3C XML, 2016) or JSON (ECMA 404 - JSON, 2013).

3.11.4. Data dictionary technical details

3.11.4.1. Data types

Data Type	Description	Example or regular expression
ARC	Administrative Reference Code (ARC) or any successive code adopted under the Excise Movement and Control System (EMCS)	'15GB0123456789ABCDEFO'
aUI	Aggregated level unique identifier coded with: either The invariant set of ISO646:1991 and composed of four blocks: (a) ID issuer's prefix in accordance with ISO15459-2:2015, (b) serialisation element in the format established by the ID issuer, (c) tobacco facility identifier code following the Data Type: FID and (d) timestamp following the Data Type: Time(s) or The invariant set of ISO646:1991 forming a code structured in accordance with ISO15459-1:2014 or ISO15459-4:2014 (or their latest equivalent))	
Boolean	Boolean value	<ul style="list-style-type: none"> • 0 (false/disabled) • 1 (true/enabled)
Component	A data type defined in the data dictionary	Aggregation
Country	Country name coded with ISO-3166-1:2013 alpha-2 (or its latest equivalent)	'DE'
Currency	Currency name coded with ISO 4217:2015 (or its latest equivalent)	'EUR'
Date	A UTC data in text corresponding to the following format: YYYY-MM-DD	E.g. '2017-03-31'
Decimal	Number values, decimal allowed	E.g. '1' or '22.2' or '333.33'
Email	Maximum 80 characters	^[!_a-z0-9-]+\(\.[!_a-z0-9-]+\)*@[a-z0-9-]+\(\.[a-z0-9-]+\)*\.\(([a-z]{2,3})\)\$
EOID	Economic operator identifier code corresponding to the format established by ID issuer coded with the invariant set of ISO646:1991	
FID	Tobacco facility identifier code corresponding to the format established by ID issuer coded with the invariant set of ISO646:1991	
Integer	Rounded number values, no decimal numbers	E.g. '1' or '22' or '333'
IIID	ID Issuer code in line with the issuing agency codes of ISO/IEC 15459	E.g. 'FTR'
ITU	Individual transport unit code (e.g. SSCC) generated in accordance with ISO15459-1:2014 (or its latest equivalent)	'001234560000000018'
List	Must be only one of the values present in the 'Values' column	
MID	Machine identifier code corresponding to the format established by ID Issuer coded with the invariant set of ISO646:1991	
MRN	Movement Reference Number (MRN) is a unique customs registration number. It contains 18 digits and is composed of the following elements: (a) last two digits of the year of formal acceptance of export movement (YY), (b) country name coded with ISO-3166-1:2013 alpha-2 (or its latest equivalent) of the Member State to which the declaration was sent, (c) unique identifier for entry/import per year and country, and (d) check digit.	'11IT9876AB88901235'
PN	Product number – numeric identifier used in the EU-CEG system to identify product presentations (e.g. GTIN (Global Trade Identification Number) of the product)	'00012345600012'
SEED	Excise number composed of: (a) country name coded with ISO-3166-1:2013 alpha-2 (or its latest	'LU00000987ABC'

Data Type	Description	Example or regular expression
	equivalent) (e.g. 'LU') and (b) eleven alphanumeric characters, if needed, padded to the left with zeroes (e.g. '00000987ABC').	
Serial	Number corresponding with the invariant set of ISO646:1991 used for serialisation	
SSCC	SSCC-18 container code generated in line with ISO6346:1995 (or its latest equivalent)	'001234560000000018'
Text (X)	Alphanumeric values coded with ISO8859-15:1999 limited to X characters	E.g. 'Abcd' or '123455588845'
Time(s)	UTC (Coordinated Universal Time) time in the following format: YYMMDDhh	'19071619'
TimeShift(s)	UTC (Coordinated Universal Time) time in the following format: YYMMDD, followed by two digits corresponding to the production shift	'190716C4'
Time(L)	UTC (Coordinated Universal Time) time in the following format: YYYY-MM-DDThh:mm:ssZ	E.g. '2017-03-31T23:16:45Z'
TPID	Tobacco Product Identifier (TP-ID) – numeric identifier used in the EU-CEG system in the format: NNNNN-NN-NNNN	'02565-16-00230'
upUI(L)	Unit packet level unique identifier coded with the invariant set of ISO646:1991 and composed of three blocks: (a) ID Issuer's prefix in line with ISO15459-2:2015, (b) middle block in the format established by ID Issuer and (c) timestamp following the Data Type: Time(s) or TimeShift(s)	
upUI(s)	Unit packet level unique identifier coded with the invariant set of ISO646:1991 and composed of two blocks: (a) ID Issuer's prefix in line with ISO15459-2:2015 and (b) serialisation element in the format established by ID issuer (i.e. UI made visible in the human readable format on the unit packets)	

3.11.4.2. Priority types

There are multiple types of mandatory/optional fields in the current system as noted in the table below.

Type	Explanation
Mandatory (M)	The variable must be completed.
Optional (O)	The variable is for optional fields which could be filled depending on the record status or type.

3.11.4.3. Cardinality Types

Type	Explanation
Simple (S)	Single value
Multiple (M)	Multiple values

3.11.4.4. Data dictionary entities details

3.11.4.4.1. EconomicOperator

EconomicOperator					
Field	Description	Data Type	Cardinality	Priority	Values
EO_ID	Economic operator identifier	EOID	S	M	

EconomicOperator					
Field	Description	Data Type	Cardinality	Priority	Values
	code. This number shall be unique at EU level.				
EO_CODE	Confirmation code in response to the registration request. It is generated by the ID Issuer solution.	Text(20)	S	M	
EO_CreationDateReg	Timestamp when the registration has been accomplished	Time(L)	S	M	
EO_UpdateDateReg	Timestamp of the last change on the register	Time(L)	S	O	
Reg_Status	Status of the registration	Integer	S	M	See RegisterStatus in section 3.11.4.6
II_ID	Identification number of the ID Issuer solution that has processed the registration	IIID	S	M	
EO_Name1	Economic operator's registered name	Text(100)	S	M	
EO_Name2	Economic operator's alternative or abridged name	Text(100)	S	O	
EO_Address	Economic operator's address – street name, house number, postal code, city	Text(300)	S	M	
EO_CountryReg	Economic operator's country of registration	Country	S	M	
EO_Email	Economic operator's email address; used to inform about registration process, incl. subsequent changes and other required correspondence	Email	S	M	
VAT_R	Indication of the VAT registration status	Boolean	S	M	0 – No VAT registration 1 – VAT number exists
VAT_N	Economic operator's VAT number	Text(20)	S	M, if VAT_R = 1	
TAX_N	Economic operator's tax registration number	Text(20)	S	M, if VAT_R = 0	
EO_ExciseNumber1	Indication if the economic operator has an excise number issued by the competent authority for the purpose of identification of persons/premises	Boolean	S	M	0 – No SEED number
EO_ExciseNumber2	Economic operator's excise number issued by the competent authority for the purpose of identification of persons/premises	SEED	S	M, if EO_ExciseNumber1 = 1	
Reg_3rd	Indication if the registration is made on behalf of a retail outlet operator not involved otherwise in the tobacco trade	Boolean	S	M	0 – No 1 – Yes

EconomicOperator					
Field	Description	Data Type	Cardinality	Priority	Values
Reg_EOID	Identifier of the economic operator that acts on behalf of a retail outlet operator not involved otherwise in the tobacco trade	EOID	S	M, if Reg_3R D = 1	

This entity is populated by the ID Issuer solution when a valid request for registration/correction/de-registration of economic operator is successfully processed. A de-registration request implies a change on the register status, not a physical deletion of the information. Once the entity data is populated, the ID Issuer replicates this register to the Surveillance Data Storage, which will route it to the Primary Data Storage solutions that may require it to ensure referential integrity.

It is recommended that only functional email addresses are used within the System.

3.11.4.4.2. Facility

Facility					
Field	Description	Data Type	Cardinality	Priority	Values
F_ID	Facility identifier code	FID	S	M	
EO_ID	The identification number of the economic operator that owns this facility	EOID	S	M	
F_CODE	Confirmation code in response to the registration request. It is generated by the ID Issuer solution.	Text(20)	S	M	
F_CreationDateReg	Timestamp when the registration has been accomplished	Time(L)	S	M	
F_UpdateDateReg	Timestamp of the last change on the register	Time(L)	S	O	
Reg_Status	Status of the registration	Integer	S	M	See RegisterStatus in section 3.11.4.6
II_ID	Identification number of the ID Issuer solution that has processed the registration	IIID	S	M	
F_Address	Facility address – street name, house number, postal code and city	Text	S	M	
F_Country	Facility country	Country	S	M	See Country in section 3.11.4.6
F_Type	Type of facility	Integer	S	M	See FacilityType in section 3.11.4.6
F_Type_Other	Description of other facility type	Text	S	M, if F_Type = 4	
F_Status	Indication if a part of the facility has a tax (excise) warehouse status	Boolean	S	M	0 – No 1 – Yes

Facility					
Field	Description	Data Type	Cardinality	Priority	Values
F_ExciseNumber1	Indication if the facility has an excise number issued by the competent authority for the purpose of identification of persons/premises	Boolean	S	M	0 – No SEED number
F_ExciseNumber2	Facility's excise number issued by the competent authority for the purpose of identification of persons/premises	SEED	S	M, if F_ExciseNumber1 = 1	
Reg_3RD	Indication if the registration is made on behalf of a retail outlet operator not involved otherwise in the tobacco trade	Boolean	S	M	0 – No 1 – Yes (possible only if F_Type = 3)
Reg_EOID	Identifier of the economic operator that acts on behalf of the retail outlet operator not involved otherwise in the tobacco trade	EOID	S	M, if Reg_3RD = 1	

This entity is populated by the ID Issuer solution when a valid request for registration/correction/de-registration of facility is successfully processed. A de-registration request implies a change on the register status, not a physical deletion of the information. Once the entity data is populated, the ID Issuer replicates this register to the Surveillance Data Storage, which will route it to the Primary Data Storage solutions that may require it to ensure referential integrity.

3.11.4.4.3. Event

Event					
Field	Description	Data Type	Cardinality	Priority	Values
Event_ID	Internal identification number of this event	Integer	S	M	
State_ID	The state of the event	EventState ID	S	M	See EventState in section 3.11.4.6
Type_ID	The type of the event	EventType ID	S	M	See EventType in section 3.11.4.6
Sender_ID	The sender who generates the event	EOID	S	M	
Event_Time	Date and Time when the event occurs	Time(L)	S	M	
Record_Time	Date and Time when the event was recorded	Time(L)	S	M	
Content	Full content of the event. According to the event type, this field will contain the proper event specific schema detailed in section 3.5.2.	Component	S	M	

3.11.4.4.4. EventNotification

EventNotification					
Field	Description	Data Type	Cardinality	Priority	Values
Event_ID	The identification number of an event involving a notification	Event ID	S	M	
Notification_ID	The identification number of the notification	Notification ID	S	M	

3.11.4.4.5. ManufacturingMachine

ManufacturingMachine					
Field	Description	Data Type	Cardinality	Priority	Values
M_ID	The identification number of the manufacturing machine. This number is issued by the ID Issuer solution, which shall ensure that the combination of M_ID, F_ID and EO_ID is unique at EU level.	MID	S	M	
F_ID	The identification number of the facility that owns this machine	FID	S	M	
M_CODE	Confirmation code in response to the registration request. It is generated by the ID Issuer solution	Text(20)	S	M	
M_CreationDateReg	Timestamp when the registration has been accomplished	Time(L)	S	M	
M_UpdateDateReg	Timestamp of the last change on the register	Time(L)	S	O	
Reg_Status	Status of the registration	Integer	S	M	See RegisterStatus in section 3.11.4.6
II_ID	Identification number of the ID Issuer solution that has processed the registration	IIID	S	M	
M_Producer	Machine producer	Text(20)	S	M	
M_Model	Machine model	Text(20)	S	M	
M_Number	Machine serial number	Text(20)	S	M	
M_Capacity	Maximum capacity over 24-hour production cycle expressed in unit packets	Integer	S	M	

This entity is populated by the ID Issuer solution when a valid request for registration/correction/de-registration of manufacturing machine is successfully processed. A de-registration request implies a change on the register status, not a physical deletion of the information. Once the entity data is populated, the ID Issuer replicates this register to the Surveillance Data Storage, which will route it to the Primary Data Storage solutions that may require it to ensure referential integrity.

3.11.4.4.6. Notification

Notification					
Field	Description	Data Type	Cardinality	Priority	Values
Notification_ID	Internal identification number	Integer	S	M	
Type_ID	The type of the notification	Notification Type ID	S	M	See NotificationType in section 3.11.4.6
Active	Qualifier that informs if the notification is still active or not	Boolean	S	M	
Creation_Time	Date and Time when the notification has been created	Timestamp	S	M	
Message	Notification message which informs about the details of what is notified	Text(512)	S	M	

3.11.4.4.7. TobaccoProduct

TobaccoProduct					
Field	Description	Data Type	Cardinality	Priority	Values
Tobacco_Product_ID	Internal identification number. This number is generated by the ID Issuer and its size is optimised according to the rules detailed in 2.1.1.4.	Text(4)	S	M	
TP_ID	Tobacco Product Identifier (TP-ID) – numeric identifier used in the EU-CEG system in the format: NNNNN-NN-NNNN	TPID	S	M	
P_Type	Type of tobacco product	Integer	S	M	See TobaccoProductType in section 3.11.4.6
P_OtherType	Description of other type of tobacco product	Text	S	M, if P_Type = 12 (other tobacco product)	
P_Brand	Brand of tobacco product	Text	S	M	
Description	The description of the tobacco product	Text(100)	S	O	
Identifier	Additional identifier used to refer to the product (e.g. GTIN or other identification number provided by the manufacturer)	Text(20)	S	O	

TPIDs are self-generated by the EU-CEG system. They are required for any product placed on the EU market. Currently, there is no available automatic data export tool from

the EU-CEG system to the Tracking and Tracing System, but the competent authorities will have access to both systems and both systems can be queried with TP-ID.

This entity is populated, if necessary, by the Surveillance Data Storage when the issuance of codes at unit packet level is notified by the ID Issuer solution. Later, when the Primary Data Storage receives the same code issuance notification from the Repository Router, the Primary Data Storage shall also populate this register.

3.11.4.4.8. TobaccoProductItem

TobaccoProductItem					
Field	Description	Data Type	Cardinality	Priority	Values
Unique_Identifier_ID	The identification code (i.e. unique identifier) of the product item as required by Article 15(2)	upUI(L)	S	M	
Tobacco_Product_ID	The identification code of the product	TobaccoProduct ID	S	M	
Manufacturer_ID	Identifier of the manufacturer of this tobacco product	EOID	S	M	
Importer_ID	The identifier of the importer into the Union, if applicable	EOID	S	O	
Manufacturing_M_ID	The identifier of the manufacturing machine	Manufacturing_Machine MID	S	M	
Facility_ID	The identifier of the manufacturing facility. This date is the one used for requesting the issuance of codes.	Facility FID	S	M	
Intended_Market	Intended country of retail sale	Country	S	M	
Intended_Route1	Indication if the product is intended to be moved across country borders with terrestrial transport	Boolean	S	M	0 – No 1 – Yes
Intended_Route2	The first country of terrestrial transport after the product leaves the Member State of manufacturing or the Member State of importation	Country	S	M, if Intended_Route1 = 1	
Import	Indication if the product is imported into the EU	Boolean	S	M	0 – No 1 – Yes
Date_Manuf	Date of manufacturing. This date is the one used for requesting the issuance of codes	Time(s)	S	M	
Serial	Serial number provided by the ID Issuer	Serial	S	M	
UI_short	Short unique identifier	upUI(s)	S	O	

TobaccoProductItem					
Field	Description	Data Type	Cardinality	Priority	Values
Application_Facility	Identifier of the facility where the unique identifier was applied	FID	S	O	

This entity, along with the UniqueIdentifier, is populated by the Surveillance Data Storage when the issuance of codes at unit packet level is notified by the ID Issuer solution. Later, when the Primary Data Storage receives the same UI issuance notification from the Repository Router, if the correct manufacturer/importer is referenced, the Primary Data Storage shall also populate this register.

Later, when the UI application event is received, the UI_short and Application_Facility fields may be updated, if available.

3.11.4.4.9. UniqueIdentifier

UniqueIdentifier					
Field	Description	Data Type	Cardinality	Priority	Values
Unique_Identifier_ID	Unique identifier of the unit packets or aggregated packaging level	Text(50)	S	M	
State_ID	The state of the unique identifier	UniqueIdentifierState ID	S	M	See UniqueIdentifierState in section 3.11.4.6
Type_ID	The type of the unique identifier	UniqueIdentifierType ID	S	M	See UniqueIdentifierType in section 3.11.4.6
Requestor_Generation_Time	Date and Time when the generation was requested	Time (L)	S	M	
Requestor_Usage_Time	Date and Time when the generator intends to use it	Time (L)	S	M	
Issuer_Notification_Time	Date and Time when the generation was notified to the storage	Time(L)	S	M	
Parent_ID	The identifier of the parent element that contains this item	UniqueIdentifier ID	S	O	
Recording_Compliance_App	Identifier of the recording compliance when applying the unique identifier	Integer	S	O	See RecordingComplianceForApplicationType in section 3.11.4.6
Recording_Compliance_Agg	Identifier of the recording compliance for aggregation	Integer	S	O	See RecordingComplianceForType in section 3.11.4.6

This entity is firstly populated, along with the TobaccoProductItem, by the Surveillance Data Storage, which creates the basic register of this entity when a notification of issuance of codes is received by the ID Issuer solution. Next, when the Primary Data Storage receives the same UI issuance notification from the Repository Router, if the

proper manufacturer/importer is referenced, the Primary Data Storage shall also populate this register.

Later, this entity is updated by the Primary Data Storage when the unique identifier application and aggregation events are processed.

3.11.4.4.10. UniqueIdentifierEvent

UniqueIdentifierEvent					
Field	Description	Data Type	Cardinality	Priority	Values
Unique_Identifier_ID	The identification number of a unique identifier involved in the event	UniqueIdentifier ID	S	M	
Event_ID	The identification number of the event	Event ID	S	M	

3.11.4.4.11. UniqueIdentifierNotification

UniqueIdentifierNotification					
Field	Description	Data Type	Cardinality	Priority	Values
Unique_Identifier_ID	The identification number of a unique identifier involved in the notification	UniqueIdentifier ID	S	M	
Notification_ID	The identification number of the notification	Notification ID	S	M	

3.11.4.4.12. Entities related to lookup tables that support the decoding of the unique identifier elements

This section includes the data dictionary entities that host the necessary information that facilitates the readability of the unique identifier elements.

On one hand, there are some entities for which registers are pre-loaded because the potential combinations are known in advance (i.e. ShipmentRouteAndMarket). On the other hand, the registers of other entities (i.e. Importer, ManufacturingActivitiesLocation and ProductDescription) are created/updated when the Surveillance Data Storage receives the registration.

The Surveillance Data Storage will act as the common data repository where the complete set of registers of these entities will be hosted. Competent authorities will use the Surveillance Data Storage as the central gateway to synchronise the necessary lookup data into their client hand-held devices.

Importer

Importer					
Field	Description	Data Type	Cardinality	Priority	Values

Importer					
Field	Description	Data Type	Cardinality	Priority	Values
Code	The identification number of the record. This number is issued by the Surveillance Data Storage solution according to the rules detailed in 2.1.1.4.	Text(3)	S	M	
Description	The description of the importer. (Synchronised from EconomicOperator.Economic_Operator_Name1)	Text(25)	S	M	
Identifier	Additional identifier used to refer to the importer. (Synchronised from EconomicOperator.EOID)	Text(10)	S	O	

This entity is populated, if necessary, by the Surveillance Data Storage when the registration/correction/de-registration register of an economic operator, which is an importer, is replicated by the ID Issuer solution. The Surveillance Data Storage will route the register to the Primary Data Storage solutions that may require it to ensure referential integrity.

ManufacturingActivitiesLocation

ManufacturingActivitiesLocation					
Field	Description	Data Type	Cardinality	Priority	Values
Code	The identification number of the record. This number is issued by the Surveillance Data Storage solution according to the rules detailed in 2.1.1.4.	Text(4)	S	M	
Reg_Status	Status of the record	Integer	S	M	See RegisterStatus in section 3.11.4.6
Machine_Ref	The reference number, or machine name, used by the economic operator. (Synchronised from ManufacturingMachine.M_Prod ucer+ManufacturingMachine.M_Model+ ManufacturingMachine.M_Nu mber)	Text(60)	S	M	
Manufacturing_Facility	The description of the manufacturing facility. (Synchronised from Facility.F_Address)	Text(60)	S	M	
Country_Of_Or igin	The description of the country of origin. (Synchronised from Facility.F_Country)	Country	S	M	

This entity is populated, if necessary, by the Surveillance Data Storage when the registration/correction/de-registration register of an

EconomicOperator/Facility/ManufacturingMachine is replicated by the ID Issuer solution. The Surveillance Data Storage will route the register to the Primary Data Storage solutions that may require it to ensure referential integrity.

ProductDescription

ProductDescription					
Field	Description	Data Type	Cardinality	Priority	Values
Code	The identification number of the record. This number is issued by the Surveillance Data Storage solution according to the rules detailed in 2.1.1.4.	Text(4)	S	M	
Description	The description of the tobacco product. (Synchronised from TobaccoProduct.Description or (TobaccoProduct.P_Brand + TobaccoProduct.P_Type)	Text(100)	S	M	
Identifier	Additional identifier used to refer to the product. (Synchronised from TobaccoProduct.Identifier)	Text(15)	S	O	

This entity is populated, if necessary, by the Surveillance Data Storage when the issuance of codes at unit packet level is communicated by the ID Issuer solution. The Surveillance Data Storage will route the register to the Primary Data Storage solutions that may require it to ensure referential integrity.

Currently, it should be noted that the product description is not provided to the System. Thus, if no description is available at the TobaccoProduct entity, the description should be retrieved from other fields (e.g. brand, product type, etc.).

ShipmentRouteAndMarket

ShipmentRouteAndMarket					
Field	Description	Data Type	Cardinality	Priority	Values
Shipment_Route_And_Market ID	The identification number of the record	Text(3)	S	M	
Route	The description of the shipment route	Country	S	M	
Market_of_sale	The description of the market of sale	Country	S	M	

The ShipmentRouteAndMarket entity is pre-loaded by the solution provider since the potential combinations can be known in advance. This entity is responsible for encoding in an optimised way and according the rules detailed in 2.1.1.4, namely the intended shipment route and the market of sale.

3.11.4.5. Canonical data model details

3.11.4.5.1. CanonicalDataModel

CanonicalDataModel					
Field	Description	Data Type	Cardinality	Priority	Values
Version	Version of the canonical data model	Text(10)	S	M	
Unique_Identifiers	List of UniqueIdentifier entity records	UniqueIdentifier	M	O	
Events	List of Event entity records	Event	M	O	
Notifications	List of Notification entity records	Notification	M	O	
Lookup_Tables	Component comprising all the information of the lookup tables (i.e. LookupTables component)	LookupTables	S	O	

3.11.4.5.2. LookupTables

LookupTables					
Field	Description	Data Type	Cardinality	Priority	Values
Manufacturing_Activities_Locations	List of ManufacturingActivitiesLocation entity records	ManufacturingActivitiesLocation	M	O	
Product_Descriptions	List of ProductDescription entity records	ProductDescription	M	O	
Shipment_Route_And_Market	List of ShipmentRouteAndMarket entity records	ShipmentRouteAndMarket	M	O	
Importers	List of Importer entity records	Importer	M	O	

3.11.4.6. Master data types

This section includes the description of the entities that comprise the master data of the Tracking and Tracing System. These entities do not change and are used to identify unambiguously the options that shall be managed (e.g. state types, countries, etc.).

3.11.4.6.1. Country types

Value	Name
AT	Austria
BE	Belgium
BG	Bulgaria
HR	Croatia
CY	Cyprus
CZ	Czech Republic
DK	Denmark
EE	Estonia

Value	Name
FI	Finland
FR	France
DE	Germany
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
LV	Latvia
LT	Lithuania
LU	Luxembourg
MT	Malta
NL	Netherlands
PL	Poland
PT	Portugal
RO	Romania
SK	Slovakia
SI	Slovenia
ES	Spain
SE	Sweden
GB	United Kingdom

3.11.4.6.2. DeactivationReasonType Types

This entity includes the list of the different deactivation reasons managed by the System.

Value	Name
1	Product destroyed
2	Product stolen
3	UI destroyed
4	UI stolen
5	UI unused
6	Other

3.11.4.6.3. EventState Types

This entity includes the different states that an event can be promoted to. The state depends on the processing stage of the event within the System.

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

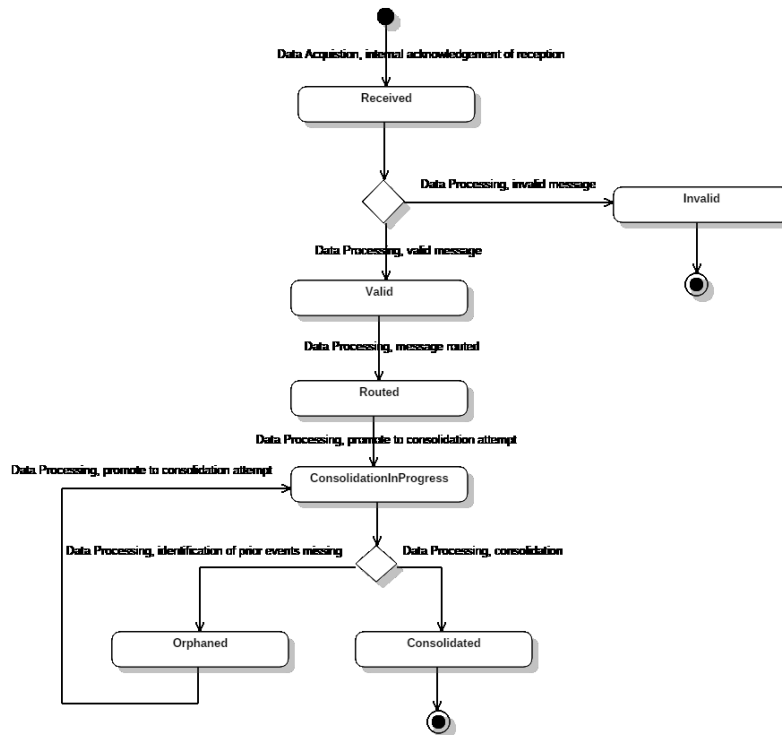


Figure 12: Event state diagram

Value	Name	Description
1	Received	Initial state. The Data Acquisition component has just received the event and stores it.
2	Valid	The Data Processing component has verified that the format and contents are correct.
3	Invalid	The Data Processing component has found some issues regarding the format or the contents. Event is promoted to invalid for further analysis by the storage provider.
4	Routed	The Data Processing component has routed (or copied) successfully the event to the other Data Storage.
5	ConsolidationInProgress	The Data Processing attempts to consolidate the information included in the event, if possible.
6	Consolidated	If the consolidation has been done, it is then promoted to <i>Consolidated</i> .
7	Orphaned	If the consolidation has not been possible because some prior events were missing, it is promoted to <i>Orphaned</i> .
8	Cancelled	Final state if the System receives a recall message regarding this event.

3.11.4.6.4. EventType Types

This entity includes the different types of events supported by the System according to the business processes.

Value	Name
EUA	Operational - UID application event
EPA	Operational - Aggregation
EDP	Operational - Dispatch
ERP	Operational - Reception

Value	Name
ETL	Operational - Trans-loading
EUD	Operational - Report an UID disaggregation
EVR	Operational - Report the delivery carried out with a vending van to retail outlet
EIV	Transactional - Invoice
EPO	Transactional - Purchase order
EPR	Transactional - Payment record
RCL	Recall - Message recall
IDA	Issuance of codes – UID deactivation
IRU	Issuance of codes – Notify the issuance of codes at unit packet level
IRA	Issuance of codes – Notify the issuance of codes at aggregated level

3.11.4.6.5. FacilityType types

This entity includes the different facility types of the economic operators.

Value	Name
1	Manufacturing site with warehouse
2	Standalone warehouse
3	First retail outlet
4	Other

3.11.4.6.6. InvoiceType types

This entity includes the different types of invoices managed by the System.

Value	Name
1	Original
2	Correction
3	Other

3.11.4.6.7. NotificationType types

This entity includes the different types that a notification can refer to.

Value	Name	Description
1	Informative	The notification only includes descriptive information, but not related to any error or abnormal situation.
2	Warning	The notification includes information about some alert or warning to be considered.
3	Alarm	The notification includes information about some alarm triggered by the System.
4	InternalError	The notification includes information about some error that has occurred within the System.
5	Other	The notification includes information about some other situation, not listed above, that has occurred within the System.

3.11.4.6.8. PaymentType types

This entity includes the different payment types managed by the System.

Value	Name
1	Bank transfer
2	Bank card
3	Cash
4	Other

3.11.4.6.9. RecallReasonType types

This entity includes the different reasons why a message recall is requested.

Value	Name
1	Reported event did not materialise
2	Message contained erroneous information
3	Other

Note: Recall reason 1 only can be used to dispatch and trans-loading events.

3.11.4.6.10. RecordingComplianceType types

This entity includes the different exception types that may occur when recording an event message not related to UI application (e.g. dispatch or arrival).

Value	Name
1	Yes – complete and a timely recording
2	No – recording delayed

3.11.4.6.11. RecordingComplianceForApplicationType types

This entity includes the different exception types that may occur when recording the UI application event or the aggregation event messages.

The exception indicates whether the UI application event message recording followed the rules for the maximum prescribed delay (i.e. the timestamp, which is a part of upUI(L), should not differ by more than the legally prescribed delay from Recording_Time, provided that the transmission of the message occurs instantaneously after the recording).

Value	Name
1	Yes – complete and a timely recording
2	No – recording delayed due to production line/machine failure
3	No – recording delayed due to problems with UI application process
4	No – recording delayed due to problems with UI verification process
5	No – recording delayed due to other reasons

3.11.4.6.12. RegisterStatus types

This entity includes the different statuses of a registered register (i.e. EconomicOperator, Facility and ManufacturingMachine) that are managed by the System.

Value	Name
1	Registered
2	De-registered

3.11.4.6.13. TobaccoProductType types

This entity includes the different types of tobacco products.

Value	Name
1	Cigarette
2	Cigar
3	Cigarillo
4	Roll your own tobacco
5	Pipe tobacco
6	Waterpipe tobacco
7	Oral tobacco
8	Nasal tobacco
9	Chewing tobacco
10	Herbal product for smoking
11	Novel tobacco product
12	Other

3.11.4.6.14. TransportMode types

This entity includes the different means of transport used when dispatching tobacco products.

Value	Name
1	Road transport
2	Rail transport
3	Water transport
4	Air transport
5	Other

3.11.4.6.15. UniqueIdentifierState types

This entity includes the different states that a unique identifier can be promoted to. The state depends on what actually occurs in the physical world to that unique identifier.

According to the business processes (Section 1.3 of this Annex), the UniqueIdentifier entity follows the state flow depicted below:

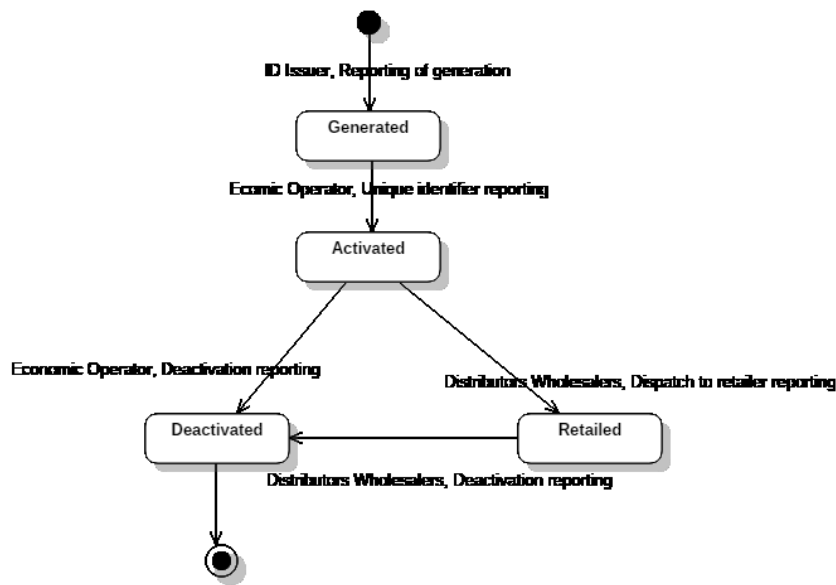


Figure 13: Unique identifier state diagram

Value	Name	Description
1	Generated	Initial state of the unique identifier. The ID Issuer reports the issuance of some codes and the Surveillance Data Storage creates a unique identifier record with the initial state (i.e. Generated).
2	Activated	The unique identifier, after being verified by the manufacturer, matches one unique identifier stored in the Surveillance Data Storage under the status "Generated". Additionally, the information contained in the date element of information matches the valid activation date for that unique identifier.
3	Deactivated	The manufacturer reports the deactivation of that unique identifier. Other cause of deactivation is when manufacturers tries to activate a unique identifier whose date element of information does not match the valid activation date for that unique identifier.
4	Expired	The Surveillance Data Storage promotes to "Expired" the codes that have been issued, but their activation has not been reported within a certain period of time (i.e. expiration time).
5	Delivered	The distributor or wholesaler reports that this tobacco product item has been successfully dispatched to the final retailer.

3.11.4.6.16. UniqueIdentifierType Types

This entity includes the different types that a unique identifier can be associated with.

Value	Name	Description
1	UnitPacket	Unique identifier at unit packet level
2	AggregatedPackaging	Unique identifier at aggregated packaging level

3.12. Common validation rules for the data

At minimum, the following rules (i.e. technical and supply chain related) shall be considered by any independent third party data storage provider, of either the Primary Data Storage or the Surveillance Data Storage:

- Supply chain:
 - Issuance of codes reporting:
 - Expiration of codes. The codes that have been issued by an ID Issuer, but their activation has not been reported within a certain period of time, should be promoted to the “Expired” status.
 - Unique identifier reporting:
 - The validity of each unique identifier referred to in the report shall be verified, namely:
 - It is already known by the storage;
 - It has a status of “generated”;
 - The primary information known by the data storage matches the primary information encoded in the unique identifier;
 - The location from where it is reported (i.e. manufacturing facility) matches the location of the primary information.

When all these verifications have been completed, the data storage shall record the secondary information that is encoded in the unique identifier and update the status of the unique identifier to “activated”.
 - Aggregation and disaggregation reporting:
 - All the unique identifiers referred to in the report shall be valid (i.e. known by the storage and with a status of “activated”).
 - Dispatch reporting:
 - Mandatory message elements shall be verified: trade information and list of unique identifiers dispatched.
 - All the unique identifiers referred to in the report shall be valid (i.e. known by the storage and with the status “activated”).
 - The last dispatch message before the first retail outlet shall specify that the purchaser is a “retailer” with some qualifier.
 - The unique identifiers referred to in the report shall match the ones (e.g. same number of items and same unique identifiers) included in the related verification (manufacturers or importers) or receipt (distributors and wholesalers) report.
 - Receipt reporting:
 - Mandatory message elements shall be verified: trade information and list of unique identifiers received.
 - All the unique identifiers referred to in the report shall be valid (i.e. known by the Data Storage and with the status “activated”).

- The report shall refer to a known dispatch event.
- The unique identifiers referred to in the report shall match the ones (e.g. same number of items and same unique identifiers) included in the related dispatch report.
- The trade elements (e.g. invoice, order number, payment record and purchaser identity) referred to in the report shall match the same trade information included in the related dispatch report.
- Individual reporting (i.e. dispatch, reception, aggregation, or disaggregation events) may be received from items at lower packaging level in case there is damage at the higher packaging level.
- State changes:
 - “Retailed” is the final state of the unit packet unless the retailer sends it back via a reverse logistic.
 - When the economic operators report a deactivation, it is a final state, either at a unit packet or an aggregated packaging level.
 - As a general rule, the state transition shall be compliant with the diagram depicted in section 3.11.
- The client users of the ID Issuer shall be previously authorised in order to avoid illicit trade entities from accessing valid codes.
- Whenever possible, the registration data shall be automatically verified (e.g. registration codes of related tables, additional identifiers, etc.).
- Technical:
 - The provider shall ensure the storage of the entities described in the data dictionary (see section 3.11) according to the technical details provided.
 - The provider shall verify that the inbound messages are conformant to the specifications detailed in section 3.5.1 and are compliant with the message structure detailed in section 3.5.2.
 - The provider shall ensure that the outbound messages are conformant to the specifications detailed in section 3.5.1 and are compliant with the message structure detailed in section 3.5.2.
 - The provider shall ensure that the messages and entities are properly managed according to the versioning information given.
 - The provider shall ensure that no message (i.e. inbound or outbound) is lost, even if an error occurs (e.g. software failure, hardware failure or communication failure).

Further data validation rules may be implemented by the provider(s) of the Primary Data Storage and the Surveillance Data Storage, if deemed appropriate. For instance, the following data analytics could be applied:

- The information that does not match the reception rules may feed an analytic engine that identifies patterns between economic operators, facilities, or countries.

- The information that does not match the dispatch rules may feed an analytic engine that identifies patterns between economic operators, facilities, or countries.
- When a new production shift starts, it should be verified how many issued codes have not been used. This information may feed an analytic engine that identifies patterns between manufacturers, importers or facilities.
- Verification of product volume mismatch, because there is a different input and output flow of products in the distributors and wholesalers.
- Verification of production information aggregated within the Tracking and Tracing System is equal to the production information reported at ECMS. In this way, product deviation can be found based on the ECMS tax information.
- Verification of major route inconsistencies, when the intended route differs greatly from the actual route.

Once all these rules have been verified, the storage provider should consolidate the information included in the message into the database, if possible and applicable (taking into account the potential temporal inconsistency because the events are not always reported in the same order as they occur).

3.13. Security policy

This section presents a list of information security requirements for the implementation and operation of the Data Storages that are part of the solution. These recommendations are based on the ISO/IEC 27000 family of standards, which defines the requirements for an information security management system (ISMS). All the requirements of this list are mandatory, and third party providers are expected to be compliant with the full list or to provide the EU with sufficient evidence to justify why a requirement cannot be met.

ID	Description
A. Right to Audit	
A1	External auditors who have executed a confidential agreement with the competent authorities from the Member States and the European Commission shall be permitted to access the provider site, and shall be subject to the agreement on prior notice regarding details of personnel, timelines, duration, and scope of the inspection being performed.
A2	The auditors designated by the competent authorities shall have the right to inspect the physical security environment, as well as the security processes and procedures implemented within the services provided including the following but not limited to: <ol style="list-style-type: none"> 1) Risk Management Process 2) Incident and Change Management Process 3) Vulnerability and Penetration Tests 4) System Hardening Guidelines 5) Business Continuity and Disaster Recovery Plans
A3	The auditors designated by the competent authorities shall have the right to inspect the operational processes implemented within the services provided at no additional cost to the competent authorities.

ID	Description
A4	The auditors designated by the competent authorities reserve the right to require changes to the provider’s security processes if they are found to be inadequate.
B. Operational Infrastructure	
B1	<p>The provider is required to implement physical and environmental controls to ensure the security of the operating environment. The physical protection of the service equipment and the service work area must as a minimum cover:</p> <ol style="list-style-type: none"> 1) Intruders 2) Ensuring safety of people 3) Natural disasters like floods, storms and earthquakes 4) Manmade disasters like bomb threats, cyber espionage and any other accidental or malicious activities
B2	Sites where EU data or processes are managed should comply with recognised standards like ISO 27001 for data centre premises management and security, and must comply with a recognised Information Security Management System (ISMS) standard like ISO 27002.
B3	The provider must ensure that all IT equipment used in providing services to the EU at least logically separate EU data from data of other customers.
B4	The transfer of data between the different providers must be secured end-to-end as a private link. The encryption level must be sufficient to ensure the integrity of the connection at the strongest current commercial level of encryption.
B5	The provider must respect clear separation of production, integration and development environments.
B6	Strong authentication with the use of industry standards must be used for accessing the system.
B7	User access to diagnostic and configuration tools shall be restricted to authorised system administrators.
B8	Mechanisms shall be implemented for encrypting sensitive data in storage.
B9	The provider must ensure the secure destruction of all media within the service in case of a failure or life expiry.
B10	The provider must monitor and prevent any use of unauthorised or unlicensed software.
B11	The provider must guarantee the integrity of all introduced software prior to their integration into the service environments.
B12	Baseline security requirements shall be established and applied to the implementation of (developed or purchased) software, systems and infrastructure. Compliance with security baselines requirements must be reassessed at least annually or upon significant changes.
B13	Policies and procedures shall be demonstrated for vulnerability and patch management, ensuring that vulnerabilities are evaluated and vendor-supplied

ID	Description
	security patches are applied in a timely manner.
B14	Service-level agreements shall clearly define security controls, capacity and service levels.
B15	Audit logs recording privileged user access activities, authorised and unauthorised access attempts, and other security events shall be retained. Audit logs shall be reviewed at least daily.
C. Information Management, Security and Confidentiality	
C1	All information submitted to the provider remain the property of the EU. EU information must not be provided to third parties by the provider.
C2	Production data shall not be replicated or used in non-production environments.
C3	The provider must formally acknowledge its responsibility to protect proprietary information by signing a confidentiality agreement.
C4	Timely de-provisioning, revocation or modification of user access to organisations' systems shall be implemented upon any change in status of employees, contractors or any third parties.
C5	The provider must promptly destroy all or a portion of data upon the EU's request at any time.
D. Risk Management	
D1	The provider must have an information risk management policy that is demonstrable.
D2	The provider must share the risk assessment findings and proposed remediation plans with the EU and notify the EU of any delays in meeting the agreed dates from implementing the risk management controls.
D3	Provider staff assigned to the service must receive training and regular updates on relevant risk management policies and procedures.
E. Incident Management	
E1	The provider must have a procedure covering the investigation and reporting of all information security incidents immediately to the EU.
E2	The provider must ensure that all information security incidents are properly managed at no additional cost to the EU and within a timescale to be documented.
E3	The provider must commit to full openness with the EU on the investigation and subsequent action taken following information security incidents involving the EU.
F. Business Continuity	
F1	The provider must have a defined set of procedures for action in a contingency situation.
F2	There must be a mutually agreed, detailed fall-back and recovery plan within the

ID	Description
	mitigation plan to prevent loss or corruption of EU information.
F3	Security mechanisms and redundancies shall be implemented to protect the service environment from threats, hazards and opportunities related to unauthorised access.
F4	The provider shall supply reliable technology supported by duplicate facilities onsite (primary) and offsite (secondary). There shall be sufficient capacity to cope with predicted workloads using a single facility.
F5	The provider must prepare an annual test plan describing the tests to be conducted and the test objectives.
G. Change and Evolution	
G1	The provider must notify EU of any changes that may have an effect on the information risk management of the service.
G2	The provider must have procedures in place to ensure the proper certification and acceptance of software, hardware and network products after testing.
G3	The provider must not use live or sensitive information from EU for testing purposes.

3.14. Confidentiality policy

This section presents the confidentiality policy requirements with regard to the System capability to ensure that data is not disclosed to unauthorised parties.

A realistic classification in terms of confidentiality must be defined by the System owner based on the likely consequences that unauthorised disclosure might have for the interests of the European Commission, other Institutions, the Member States, or other parties.

The requirements related to the confidentiality are described in the “Data protection” section of the requirements specification. These requirements have been included in both data storage solutions: Primary Data Storage (section 3.7.1.2.3) and Surveillance Data Storage (section 3.8.1.2.3).

3.15. Contingency plan

Section 3.13 of this document defines a security policy for all Data Storages, which are part of the solution. The sites where these Data Storages are deployed shall comply with ISO 27002 (ISO/IEC 27002:2013 Security techniques, 2013), an internationally-recognised standard of good practice for information security, requiring appropriate business continuity and disaster recovery planning to be implemented by the third party provider. Moreover, this plan must be aligned with the technical requirements defined in sections 3.7 and 3.8 for the third party Data Storages. ISO 22301 (ISO/IEC 27002:2013 Security techniques, 2013) specifies the requirements that a provider needs to comply with to obtain a certified business continuity management plan, while ISO 22313 (ISO/IEC 22313:2012 BCMS Guidance, s.f.) defines the guidelines for business continuity management systems (BCMS) that this plan must follow.

The list below presents the minimum recommended (Advisera - ISO 22301, 2016) set of artefacts and records required by ISO 22301 that shall be elaborated by the independent third party:

- Procedure for identification of applicable legal and regulatory requirements (clause 4.2.2) – defines who is responsible in the company for establishing and communicating the compliance objectives, and how these objectives will be measured and evaluated.
- List of legal, regulatory and other requirements (clause 4.2.2) – lists all legal and regulatory requirements that are applicable, and that should become compliance obligations for the company.
- Scope of the BCMS and explanation of exclusions (clause 4.3) – defines the scope of the BCMS, documenting any possible exclusion (i.e. system or data that is not covered by the business continuity management plan).
- Business continuity policy (clause 5.3) – defines main responsibilities, and the intent of the management. Includes a commitment to attend applicable requirements, and to continually review and improve the BCMS.
- Business continuity objectives (clause 6.2) – defines measurable objectives that are to be achieved with business continuity.
- Competencies of personnel (clause 7.2) – defines knowledge and skills required of people given responsibility for the BCMS who work under the organisation’s control. Identifies the experience, training and/or education regarding the assumed tasks that must be demonstrated.
- Communication with interested parties (clause 7.4) – defines all relevant interested parties (internal and external to the organisation), and the processes to communicate with them. Defines the elements that need to be recorded, who needs to receive the communication and who is responsible for starting the communication. Defines the actions needed to ensure the availability of communication resources during disruptive events.
- Process for business impact analysis and risk assessment (clause 8.2.1) – defines the methodology for analysing the adverse impacts to the organization’s products, services, and operations. The role of the business impact analysis (BIA) is to systematically identify continuity and recovery priorities and define objectives and goals to be achieved, in terms of minimal acceptable performance and time to achieve them. Risk assessment (RA) evaluates risks that may lead to disruptive situations.
- Results of business impact analysis (clause 8.2.2) – documents the results of BIA.
- Results of risk assessment (clause 8.2.3) – documents the results of RA.
- Business continuity procedures (clause 8.4.1) – include incident response, recovery and business continuity plan(s).
- Incident response procedures (clause 8.4.2) – defines the initial procedures for the activation of a proper continuity response to various incidents, including communications with relevant interested parties.
- Decision whether the risks and impacts are to be communicated externally (clause 8.4.2) – this decision is normally made by crisis manager.

- Communication with interested parties, including the national or regional risk advisory system (clause 8.4.3) – this can be documented through emails, minutes, memos, etc.
- Records of important information about the incident, actions taken and decisions made (clause 8.4.3) – normally this is done through minutes.
- Procedures for responding to disruptive incidents (clause 8.4.4) – these are the business continuity plan(s) and recovery plan(s), including the disaster recovery plans.
- Procedures for restoring and returning business from temporary measures (clause 8.4.5) – defines the procedures needed to restore and return business activities from temporary conditions, defined as achieving the minimum performance levels agreed upon for a situation of “business as usual”, operating under normal conditions.
- Results of actions addressing adverse trends or results (clause 9.1.1) – defines preventive actions in response to adverse trends.
- Data and results of monitoring and measurement (clause 9.1.1) – defines planned periodic evaluations of business continuity procedures to ensure that the BCMS meets the objectives.
- Results of post-incident review (clause 9.1.2) – defines an evaluation procedure on how effective a business continuity plan is in a real situation.
- Results of internal audit (clause 9.2) – defines the internal audits that should be performed at planned intervals, considering the processes’ relevance and the results of previous audits, to ensure compliance with the standard’s requirements and the requirements defined by the organisation itself.
- Results of management review (clause 9.3) – defines the management review that must be performed at planned intervals and at top management level to ensure the overall suitability of the BCMS.
- Nature of nonconformities and actions taken (clause 10.1) – defines a nonconformity / corrective action for each problem detected in management reviews, internal audits, and compliance and performance evaluation.
- Results of corrective actions (clause 10.1) – provides a description of what has been done to eliminate the cause of a nonconformity.

4. GLOSSARY AND TERMS OF REFERENCE

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

5. BIBLIOGRAPHY

- Advisera - ISO 22301. (2016). *Clause-by-clause explanation of ISO 22301 white paper*. Retrieved April 2017, from http://info.advisera.com/hubfs/27001Academy/27001Academy_FreeDownloads/Clause_by_clause_explanation_of_ISO_22301_EN.pdf
- apsstandard - RQL. (2014). *Resource Query Language*. Retrieved April 2017, from <https://doc.apsstandard.org/2.1/spec/rql/>
- CMT. (2017). *Comisionado para el mercado de tabacos*. Retrieved from <http://www.cmtabacos.es/wwwcmt/paginas/ES/webInicio.tpl>
- Cognex. (2013). *A guide to barcode symbology for the logistics industry*. Retrieved from http://www.abr.com/wp-content/uploads/2014/08/cognex_wp_expert_guide_symbology_040814.pdf
- Commission Delegated Regulation (EU) 2016/161 - FMD. (2015, October 2). *Falsified Medicines Directive - Delegated Act*. Retrieved January 16, 2017, from http://ec.europa.eu/health/files/eudralex/vol-1/reg_2016_161/reg_2016_161_en.pdf
- Directive 2014/40/EU of the European Parliament and of the Council. (2014, April). *Tobacco Products Directive - DIRECTIVE 2014/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*. Retrieved December 22, 2016, from http://ec.europa.eu/health/sites/health/files/tobacco/docs/dir_201440_en.pdf
- Eckstein, J. (2007). *Memory Storage Calculations*. Retrieved from <http://eckstein.rutgers.edu/mis/handouts/storage-calcs.pdf>
- ECMA 404 - JSON. (2013, October). *The JSON Data Interchange Format Standard*. Retrieved from <http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf>
- European Commission - Decision 3602. (2006, August 16). COMMISSION DECISION of 16 August 2006 C(2006) 3602. Brussels, Belgium. Retrieved April 03, 2017, from http://ec.europa.eu/internal_market/imi-net/docs/decision_3602_2006_en.pdf
- European Commission - JRC. (2017). *Best Practice Guidelines for the EU Code of Conduct on Data Centre Energy Efficiency - version 8.1*. Retrieved April 2017, from Renewable and Energy Efficiency Unit: <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC104370/2017%20best%20practice%20guidelines%20v8.1.0%20final.pdf>
- European Commission - REGULATION (EU) 2016/679. (2016, April 27). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Brussels, Belgium. Retrieved April 03, 2017, from <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1491990011093&from=en>
- everis. (2017). *D2-TTIS-Interim_Report_II-v1.00*.
- F. Ferguson, Donald; Hadar, Ethan. (2012). *Optimizing the IT business supply chain utilizing cloud computing*. Retrieved May 2017, from <http://www.isaca.org/Groups/Professional-English/governance-of-enterprise->

- it/GroupDocuments/Optimizing%20The%20IT%20Business%20Supply%20Chain%20Using%20Cloud%20Computing.pdf
- Feltus, C., Petit, M., & Sloman, M. (2010). Enhancement of Business IT Alignment by Including Responsibility Components in RBAC. Namur, Belgium. Retrieved March 07, 2017, from <https://pure.fundp.ac.be/ws/portalfiles/portal/1052109>
- GS1. (2013). *GS1 Identification Keys in Transport & Logistics*. Retrieved from http://www.gs1.org/docs/tl/T_L_Keys_Implementation_Guideline.pdf
- GS1. (2015). *GS1 Barcode Fact Sheet*. Retrieved from http://www.gs1.org/docs/barcodes/GS1_Barcodes_Fact_Sheet-Scanner_enviroments_and_printing_methods.pdf
- GS1. (2017). *GS1 General Specifications*. Retrieved from http://www.gs1.org/docs/barcodes/GS1_General_Specifications.pdf
- ISO/IEC 15459:2014 - Unique identification. (2014). *Automatic identification and data capture techniques -- Unique identification*. Retrieved May 2017, from <https://www.iso.org/standard/54779.html>
- ISO/IEC 19505-1:2012 UML. (2014, April). Information technology -- Object Management Group Unified Modeling Language (OMG UML). Retrieved January 16, 2017, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=32624
- ISO/IEC 19987:2015 EPCIS. (2016, December). Information technology - EPC Information services (EPCIS) – Specification. Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66796
- ISO/IEC 22313:2012 BCMS Guidance. (n.d.). *Business continuity management systems -- Guidance*. Retrieved from <https://www.iso.org/standard/50050.html>
- ISO/IEC 27002:2013 Security techniques. (2013). *Security techniques -- Code of practice for information security controls*. Retrieved April 2017, from <https://www.iso.org/standard/54533.html>
- OWASP - Secure Coding. (2016). *OWASP Developer Guide - Secure Coding*. Retrieved April 2017, from https://www.owasp.org/index.php/OWASP_Guide_Project
- Priyanka Gaur, S. T. (2014). *Recognition of 2D Barcode Images Using Edge Detection and Morphological Operation*. Retrieved from <http://www.ijcsmc.com/docs/papers/April2014/V3I4201499b59.pdf>
- Radyakin, S. (2016). *Survey Solutions: Lookup tables*. Retrieved from <http://siteresources.worldbank.org/INTCOMPTOOLS/Resources/8213623-1380598436379/lookup.pdf>
- Sciences, D. o. (2015). *Barcode - History and Symbology*. Retrieved from <http://www.its.fd.cvut.cz/ms-en/courses/identification-systems/idfs-02-barcodes-history.pdf>
- Supply Chain Insights. (2014). *Building Business-To-Business Supply Chain Networks*. Retrieved from http://supplychaininsights.com/wp-content/uploads/2014/04/Building_B2B_Supply_Chain_Networks-Who_Are_The_Players-24_APR_2014.pdf

- TAXUD. (2009). *EORI National Implementation*. Retrieved from http://ec.europa.eu/ecip/documents/who_is/eori_national_implementation_en.pdf
- TEC-IT. (2017). Retrieved from Barcode Overview: <http://www.tec-it.com/en/support/knowledge/barcode-overview/linear/Default.aspx>
- Tobacco1. (2017). *Importers of tobacco products in Europe*. Retrieved from <https://www.tobacco1.com/>
- University, C. S. (2011). *2D Barcode Information and Guidelines*. Retrieved from <http://www.csuci.edu/news/documents/2011-2dbarcodeinfo.pdf>
- Vignola, C. (2013, April 18). Batch Applications for the Java Platform. Retrieved March 17, 2017, from <https://jcp.org/aboutJava/communityprocess/final/jsr352/index.html>
- W3C XML. (2016, November 10). *XML specification*. Retrieved January 16, 2017, from <https://www.w3.org/XML/>

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

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

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

Priced publications:

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

