Pages 1 to 151 were entirely deleted, as they fall outside the scope of the request

Document 12.3

Justification	The disadvantages of a distributed topology are as follows: • 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 may change. Therefore, any change to 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	-

Commented [redacted] Where is this expiration time described in detail?

Table 34: 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

Pages 153 to 155 were entirely deleted, as they fall outside the scope of the request

competent authorities 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 will jointly select the third party data storage provider that will establish the Surveillance Data Storage solution.

Commented [redacted]**:** Selected or proposed? As the European Commission must approve it. And how is this selection done, by majority of the Primary Data Storage providers, unanimous or other criteria?

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 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 on 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.

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):

Pages 157 to 201 were entirely deleted, as they fall outside the scope of the 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 shall contain an RQL statement

Commented [redacted]**:** On p221 RQL is mentioned as possible solution, here it is implied as it is already as being the chosen query language.

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	

3.5.2.6.2. 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_Resp	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**

3.5.2.7. Recall messages

Request:

recall – request

Pages 203 to 277 were entirely deleted, as they fall outside the scope of the request