Ref. Ares(2019)7058576 - 14/11/2019

EU Tracking and Tracing System for tobacco products

Subject	Comments on EU Tracking and Tracing System for tobacco products
Name	
Email	
Phone	+31

Introduction

These are my comments for a new EU system for traceability and security features in the field of tobacco products. The comments are solely based on the Interim Report III second draft and after attending the expert workshop/meeting on 17th May in Brussels.
Comment are only made on the software architecture of the system, the physical security features of the system is outside my area of expertise.

High level overview of the subsystems

This is a high level summary of the software components needed to built the system:

- Surveillance data storage

- Repository router
- Primary data storage
- ID issuer
- Temporary buffer

Design and development

As has been mentioned the time frame to design and develop these systems will be approximately 17 months. Information between the different subsystems is exchanged via a predefined abstract messaging structure. If I'm correct it is not yet known which providerwill design which system. After the final report (WP4) there will be an open bid to vendors. Although the different subsystems are dependent on each other they can be designed in parallel by different providers.

Messaging layer

As described on page 188:
"The message exchange system shall be performed through a web service solution using an HTTP API (e.g. REST)
...
Messages shall be formed in XML or JSON, according with the implemented message exchange architecture."

As this is an important part of the whole system the technical design and implementation will be crucial to achieve the expected messaging throughput per subsystem. In theory each subsystem can be developed by a different vendor. The abstract message structure is already defined, but who decides how this messaging protocol will be implemented in terms of technology choice. (e.g. between ID issuer and Primary Data Storage or between Primary Data Storage and Surveillance Data Storage and vice versa)?
The broker topology already mentioned in the report (page 111) is the recommended architecture. I think it would be important for solution providers of a subsystem to discuss and agree upon a chosen technology before development. (e.g. ActiveMQ, RabbitMQ, MQTT or other technology).
In my opinion the developer of the Surveillance Data Storage should have a leading role in this.

Developer platform

I'm not aware of how the practical project management for developing the different subsystems will take place. Will the final technical requirements document be enough for a provider to independently develop a subsystem? Will there be a kickoff meeting between solution providers? If feasible setting up a developers platform may be useful for providers working on solutions to communicate with each other on a technical level. As the timeline for the technical rollout is ambitious it could be helpful in identifying and proposing solutions to

challenges during development. This platform could be controlled by the Governing Body of the Tracking and Tracing System.

Test scenarios

Functional testing

As each subsystem can be developed by a different vendor testing use cases of interaction between multiple subsystems can take a considerable amount of time. A set of predefined functional test scenarios of all possible use cases (unit and integration tests) between subsystems is recommended. Each solution provider will have test cases for their own subsystem, but who will define the integration tests of subsystems? As the surveillance data storage is the core system of the whole project it seems logical to me that the solution provider will define and create these test cases.

Security testing

In section *5.10. System security plan* (page 228) security recommendations are proposed based on standard decision 3602 and OWASP. Each solution provider will be expected to implement the security requirements into their solution.
I'm not sure if this topic is part of the tasks of the external auditor, but a suggestion would be to have a 3rd party to design security tests that can apply to each subsystem.

Technical roll-out

The roadmap for the technological roll-out is scheduled for beginning of 2018 and a production implementation of May 2019. Is it required to be a big bang roll-out for the whole system? Or is there a consideration when the time frame permits of a pre roll-out for one or more sites so that last minute issues can be identified?

Overall impression

My overall impression of the system regarding the software architecture is that the design looks solid, extensive and well thought out. The data model, abstract messaging structure, number of functionalities and features does not look complex. There are challenges in designing and implementing a datastore and message brokers that can handle massive volumes of data and messages throughput. Also managing and dealing with different system users and solution providers will be a challenging task.
Although the delivery time frame to implement the system by May 2019 seem ambitious I think it is possible to finish it in time.