Document 10.1

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

Interim Report III – Second Draft

EXPERT WORKING GROUP COMMENTS BY [redacted]

As discussed during the Expert Workshop, May 17, 2017 Brussels

1 APPROACH AND PERSPECTIVE IN RELATION TO THESE COMMENTS

Given this panelists expertise and qualifications, the primary perspective in relation to these comments is from domain knowledge with regard to illicit trade, customs and excise and related traceability technologies and solutions. Prior works by this expert and familiarity with the overall EC process also features in these comments. The other experts have much deeper skills in relation to the information technology intensive aspects (e.g., messaging, software development etc.). Thus, while these comments focus primarily on the former, given the vast expertise in building large enterprise systems, the more technical observations and comments are primarily from the strategic perspective.

These comments have been divided up into three main sections: General comments, questions or areas that lack clarity in the document; and specific citations and comments on content with page number references.

2 GENERAL COMMENTS

2.1 STRATEGIC ALIGNMENT

With any large-scale system, strategic alignment to the goals and objectives in terms of the results and benefits to be derived is paramount. At the risk of reiterating an obvious point, the premise of the TPD Article 15 and 16 which is based on the Article 8 of the Protocol is grounded on attempting to control an industry found to be complicit in the proliferation of illicit trade. The fact remains that incidents involving the large tobacco manufacturers fraudulent activities continue to occur around the world. The very premise of the system for control is based on the concept of mistrust as opposed to trust. Any solution that relies on "trusting" an industry that is commercially/economically incentivized to circumvent controls is bound to fail. From a governance and technical perspective, the solution should first and foremost be robust enough to prevent manipulation or circumvention by the tobacco industry. There are still several key elements of the solution that have not been finalized or fully developed and these are essential in determining whether or not the system will be effective. If the controls are not robust enough, and key concepts are not aligned to this essential purpose, the system has the potential to do the opposite of what it is intended to do – providing a false sense of control where detection of fraud would be nearly impossible (giving illicit production a "technical forest" in which to hide). Given the lack of resources in terms of audit and other governance controls at the disposal of the competent authorities, this is not a simple objective to achieve, but is also not impossible. Therefore, the requirements around production control, audit, anti-tampering, third-parties and the technical and governance standards that will be adopted, are critical to the potential efficacy of the solution.

Although the solution design must be compliant with the TPD, the TPD is not intended to be a system design specification. The approach of the design in many areas appears to be solely explicit driven by what the TPD does say on and not what it does not say. It is the job of solution design to provide specifications that best meet the intent of the statute. The litmus test for these specifications should be "is the requirement legal under the TPD" and not rely on the TPD for granular specificity as a basis for the requirement because it is simply not there.

2.2 GOVERNANCE MODEL

The chosen governance model (A3) still lacks the requisite specificity in terms of the activities in relation to the end-to-end system necessary to meet the requirements of the TPD and the FCTC Protocol. For example, who will make the final decisions with respect to the particulars of what each party will be responsible for (competent authority vs. industry)? A solution of this type would typically require a robust, funded and staffed entity to oversee that such a system indeed meets the standards in relation to the model itself. This would need to be supported by auditors or audit standards and guidelines. None of this specificity is currently evident in the solution design. Furthermore, who will make the decision as to "Who" the third parties will be? Will this be decided by the industry or by the competent authorities. The competent authority approving contracts is not adequate oversight. Without the requisite standards or guidelines in place, surely, any such contracts would be structured by the industry to pass this limited modicum of oversight. **The current solution design does not define or even explore the control required to ensure that the potential for collusion is minimal.**

2.2.1 Concept of Third Party

The concept of "third-party" has been used in connection with the implementation of an EU system from the start of the project. Indeed, the current governance model choice (A3) refers to a mixed solution whereby the industry and a third-party will "ensure the required level of system integrity by the allocation of various responsibilities and functions to the operators involved in the supply chain" . Based on the inherent risks associated with this choice given the historical practices of the tobacco industry, the document does not yet explain how adequate production monitoring or controls related to security features will be achieved through this 3 [d] party/manufacturer relationship (the issuing of serial numbers by a third party does not in itself ensure that undeclared/uncontrolled production does not occur). As discussed in the meeting "clones" of legitimate product could be introduced into the market simply by having access to the production environment and the security features. Commercially available security features as well as those that are difficult or even impossible to account for (e.g., digital fingerprinting) significantly amplify this risk.

The implementation analysis provides no definition for the concept of a "third-party" in relation to the envisaged EU system. As with other areas and key concepts in relation to the EU system, it is advisable as well as a common best practice to utilize pertinent standards wherever they can be applied. The use of standards is particularly important when one considers the number of role players and stakeholders that will be required to operate within the EU system. There are several standards that can be readily applied in the definition and design of the EU system. The most obvious standard in terms of the activities of the envisaged third-party is: ISO/IEC 17021: *Conformity assessment - Requirements for bodies providing audit and certification for management systems.* This standard is part of a family of standards that provide clear definitions in relation to the functions and activities that would be required of a third-party that can ensure the level of system integrity that is required. ISO 17021 specifies requirements for bodies providing audit

[1] Implementation analysis of a EU system for traceability and security features of tobacco products, Interim Report III pg. 37.

and certification of management and production systems. Observance of these requirements is intended to ensure that certification bodies providing system certification do so in a competent, consistent and impartial manner.

This standard relies on the following definitions which may be applicable to the EU system including:

- **Conformity Assessment -** demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.
- **Third-party conformity assessment activity -** conformity assessment activity that is performed by a person or body that is independent of the person or organization that provides the object, and of user interests in that object.
- **Impartiality –** the presence of objectivity by the certifying body, e.g. conflicts of interest do not exist, or are resolved so as not to adversely influence subsequent activities of the certification body. Conflicts of interest can include past history of a business relationship, shared or derived intellectual property, a financial relationship between the third-party and the subject of the oversight activity.

2.2.2 CONSIDERATION/RECOMMENDATION

Applying the pertinent ISO standards either in a *de jure* or *de facto* manner would certainly enhance the integrity of the EU system but may preclude any tobacco industry developed solution or intellectual property from being eligible. It may also preclude the use of traditional commercial suppliers to the tobacco industry.

2.3 SECURITY FEATURE OPTIONS

It is well defined in the TPD that security features are critical to the success of tobacco control in the EU. The document, (although stating that the security feature section was mainly covered by the feasibility study) did not endeavor to take the analysis further by examining more deeply which security features would be most appropriate based on the optimal system (Table 3). Indeed, the criteria utilized in the derivation of the optimal system completely ignored the 'what' security features and chose instead to focus on the 'how' method of adding a security feature, settling on the 'mixed solution' option. This ignores the obvious point that the "what" in terms of the security features themselves are far more important to the overall solution objective than the method of application which is where the emphasis has been placed. Prior comments included as justification to the Feasibility Study's chosen method of application for the security features are as follows:

The "affixing" method presented the following advantages:

- *Lowest Cost – label applicators are already installed.*
- *Highest number of security feature options available.*
- *Most number of private, independent, security feature providers.*
- *Most robust package of security features from a layering perspective and in terms of large-scale system tampering.*
- *Proven efficacy as demonstrated by tax stamp industry and other implementations related to control of illicit trade.*

- *Potential to combine with existing tax stamp programs of majority of Member States to absorb existing sunk costs in terms of applicators.*
- *The same method would be applicable across all tobacco products and related packaging (tins, bags, etc.).*

It is well-known that the tobacco industry favors its own methods and long-standing commercial partners that provide solutions that embed features and tracers into packaging in order for the industry to identify counterfeits. These, however, may not be the best fit with regard to the intent of the EU solution.

The chapter dedicated to the security feature (section 8 of the implementation analysis) does not actually provide anything close to a technical specification for the security feature(s) themselves. The security features that are listed merely provides a description of the various types of security features available and categorizes them in relation to the TPD. This was already done in the original Feasibility Study (Section 4.2 of Interim Report I). This same document also provided a basis for evaluation based on a set of criteria jointly developed and agreed with Commission staff with respect to how such features could be evaluated, vis-a-vis the problem statement. This is a logical progression in terms of providing further clarity and definition around high-level legal concepts such as "visible", "invisible" etc. IT solutions cannot be adequately designed from the level of the legislation and it is the job of solution designers to make logical and specific technical choices that are consistent with the law. The current approach has this the other way around. Indeed, under the current approach security features which are obsolete (and are highly susceptible to counterfeiting) would pass muster within the current solution design. The security feature industry is constantly evolving to stay ahead of counterfeiters. There are tax stamps that are easily counterfeited and there are those that are nearly impossible to counterfeit. At which end of this spectrum does the EU solution want to be?

A clear rationale was behind the security feature packages that were set out in the Feasibility Study. This was articulated in sections 6.6 and 7.2.2 of the First Interim Report (Annex A). This could be further updated and refined to reflect new technologies etc. and used as a basis to further evaluate and assess security features that may be appropriate for the EU solution. The Implementation Analysis does not further this critical element of the EU solution but rather goes backwards by simply providing a list of all potential security features available on the market. This is not a technical specification.

Additionally, section 7.2.2 of the First Interim Report of the Feasibility Study went into some detail regarding the efficacy of the overt and covert security features that are viable, and meet the requirements of the TPD. The current table classifying and grading security feature components (section 8.4.5) displays some subjective bias that may come under scrutiny by the various security feature stakeholders and may only serve to confuse potential decision makers. Supporting the study, and further towards utilizing standards where applicable, ISO *12931- 2012: Performance criteria for authentication solutions used to combat counterfeiting of material goods* details a process to identify appropriate authentication solutions (security features) to be utilized for certain situations and under certain circumstances.

The Feasibility Study Final Report also provided a matrix of the tax stamp programs currently employed in the EU with some details on the features present on each stamp (Annexure 4: Existing Tax Stamp Programs in EU Member States).

To conduct a more detailed analysis of the security features across the EU (out of scope for phase one) would not require a significant effort and could be done relatively quickly. This could be the basis from which to develop some minimum standards for security features for the EU solution. The "anything/everything goes" has the potential to create an inconsistent and convoluted security feature baseline without realizing any potential synergies that could be leveraged with regard to enforcement and authentication which is indeed the very purpose of the security feature in the first place.

The current solution design has made similar technical choices with respect to other aspects (e.g. data carrier standards, unique identifier etc.) so the security feature "specification" is not aligned to other solution elements and it is not in line with the overall methodology as set out in the document.

2.3.1 CONSIDERATION/RECOMMENDATIONS

- Establish specific criteria for the inclusion of security features (prior works as referenced above could serve as a starting point). **A set of minimum standards that must be adhered to when selecting security features is not only possible but essential to the integrity of the system.**
- Review the security features in the current tax stamps within the EU to see if a minimum standard already exists.
- Define a standard for each method of application. With regard to the "Affixed" method, option 1 from the Feasibility Study is potentially the best place to start.
- Clearly define what is meant by "integrating through a different method". This is important since both the TPD and Protocol state clearly that security features must be "printed on" or "affixed to", thus the legality of this yet to be defined method is questionable.

2.4 ILLICIT TRADE IN TOBACCO FRAUD ARCHETYPES VS CURRENT SOLUTION DESIGN

2.4.1 Export Fraud

Production for export is a well-known and long-standing risk that is often exploited by illicit traders. A report by the EC: *Progress report on the implementation of the Commission Communication "Stepping up the fight against cigarette smuggling and other forms of illicit trade in tobacco products - a comprehensive EU strategy (Com (2013) 324 final of 6.6.2013)*" found that one of the common smuggling scenarios used is that cigarettes are produced inside the EU and declared for export but are actually not exported at all or are smuggled back in the EU after export. This can be done with or without the tobacco manufacturers knowing collaboration. Within the parameters of the TPD and other relevant statutes, the EU solution should explore this scenario further to understand and specify how the track and trace solution might contribute to mitigating this risk. Although the Tobacco Products Directive does not explicitly proscribe track and trace and security features for export related production, it does explicitly imply that the production of tobacco in, and imports to, the EU should be controlled. TPD states that "*Member States shall ensure that all economic operators involved in the trade of tobacco products, from the manufacturer to the last economic operator before the first retail outlet, record the entry of all unit packets into their possession, as well as all intermediate movements and the final exit of the unit packets from their possession".* The legal question on this is if exports is considered as "involved in the trade". Ideally, the recording of goods manufactured for export could form part of the "verification" step both on the

production line and potentially at exit from the manufacturers premises. This would contribute to closing the gap related to exports. Not closing this gap within the EU solution would be a missed opportunity and leave the door open to this type of fraud.

2.4.2 Illicit Trade Archetypes

As stated in prior comments, a vulnerability assessment should be conducted once the final solution design is complete. The following provides a high-level analysis of the current solution vis-à-vis typical illicit fraud topologies. It is not intended to be an exhaustive list.

Risk Archetype	Does the solution address this archetype?
Smuggling of unmarked packs: Scenario: Unmarked goods are produced outside of the EU and sold within one of the member states.	As the document does not provide specifications for enforcement procedures it is difficult to anticipate how this risk will be mitigated, however, a track and trace solution with security features will provide enough information for an enforcement officer to distinguish whether a pack is legitimate in the EU territory or not. From a border control perspective, this can be controlled upon entry into any of the member state borders. From a local (within member state territory) perspective, this can be controlled using enforcement procedures.
Illicit production of branded products (counterfeiting): Scenario: refers to 'unregistered' manufacturers producing branded products for sale within the territory.	In order for the unregistered manufacturers to reproduce legitimate, branded products they would need to copy the UID and the security features of the legitimate goods. Copying the UID could be achieved by simply purchasing a shipment of legitimate goods and duplicating the UID's on these goods or by gaining access to the data store at the various levels (e.g., buffer, production line, central data storage). Given the value of this data in terms of the ability to translate into a highly profitable trade in illicit products, this is a risk. This risk can be mitigated considerably by ensuring that the security feature(s) are robust and not easily duplicated or otherwise compromised. Access to security features and their raw materials should be tightly controlled.

Fraudulent 'legitimate' production: Scenario: This refers to registered manufacturers employing 'third shift' or unrecorded manufacturing of legitimate products within the EU.	The solution does not include or propose any mechanism of production monitoring or control with regard to the production lines themselves. Based on the solution design, a manufacturer requests an UID from a 3 [d] party and then applies these to packs. Following this, the design allows for either 3 [d] party integration control or manufacturer control of SF. The solution design however, does not prescribe a minimum standard or specification for the SF, leaving it up to the MS or designated 3 [d] party to decide. Assuming the SF may be compromised, a manufacturer can duplicate these UID's and distribute them into the market as legitimate, and there will be no effective means of identifying this risk as it would only become prevalent if both the original and the duplicate are intervened through enforcement means. Depending on the sophistication of the distribution channel, the likelihood of these duplicated packs being identified once they have left the manufacturer is slim.
Round Tripping: Scenario: Goods produced and exported are smuggled back into the territory.	The scope of the solution design does not cater for any kind of export controls, implying that the production of these goods may never be recorded by the system. Additionally, these goods may not be tracked and traced or have security features. In terms of 'legitimate' sales control, this risk is mitigated as the products will be easily identifiable and will therefore not be purchased or sold. However, in terms of 'illegitimate' sales control this risk remains as these products will still be sold 'under the counter' to willing buyers. Small scale versions of this fraud (e.g., small shipments in vehicles, travelers, etc.) is nearly impossible to prevent entirely. The practice of flooding low-tax foreign markets with more tobacco than they are capable of consuming has been a common practice used to supply illicit trade. There is a current case brought forth by HMRC against BAT (fined 650,000 pounds for oversupplying the Belgian market[2]).

2.5 DOCUMENT PURPOSE AND STRUCTURE

The document is intended as an implementation framework related to the technical specifications for the implementation of an EU system for traceability and security features (hereinafter, "EU system"). Accordingly, one would expect that it would provide clarity with regard to all of the necessary components of the EU system in terms of governance, design, maintenance and management. The table of contents further encourages these expectations.

However, the actual content does not specify the requirements to an adequate level of detail to be deemed a specification, in fact, leaving much open to interpretation. While it may be advantageous in

[2] https://www.theguardian.com/business/2014/nov/16/bat-fined-for-oversupplying-tobacco-in-low-tax-european-jurisdictions

some respect to have a degree of 'free-reign', this approach could potentially result in incongruous technological solutions being selected by independent entities (manufacturer, Member State, etc.). This inherently presents potential challenges for the effective integration required for oversight and functioning of the EU solution. It would require, for example, that the centralized (surveillance) database be robust enough to cater for varying methods of integration with the differing solutions, adding a level of complexity that can be avoided by providing a set of standards or 'implementable' guidelines that should serve as a detailed blueprint for any entity when selecting their solution.

This document does provide sufficient detail and many of the required design artefacts (process flows, use cases, etc.) but not across the full spectrum of the solution. This specificity is lacking particularly in, but not limited to, the following areas:

- Guidelines or standards defining the selection criteria of security features;
- Procurement and application of such security features;
- Accreditation and auditing in relation to 3 ^{d} party activities (UID, security features, verification);
- User requirements for the key non-industry stakeholders (e.g. customs, revenue and enforcement officials);
- Integration standards or governance methods;
- Enforcement and risk mitigation activities;
- Considerations with regard to tobacco products manufactured in the EU for export.

Some observations and points to consider in this regard:

1. The document touches on the architecture and implementation but lacks the descriptive overviews and corresponding detail that would provide the necessary direction on the design.
2. The SDLC covered within provides a very generic and general view of how any IT implementation would be conducted. This needs to be followed through with the detailed layout of each phase related to the specific solution, whether it be included within the same document or referenced to related documents for each phase.
3. There needs to be a clear distinction between the business, functional and technical requirements along with a collective mapping of their relationship in realizing the solution and ensuring that all aspects are catered for. A requirements traceability matrix will aid in mapping, aligning and maintaining both a link and reference to each of these. In addition, the matrix should be complex enough to reference a specific requirement's occurrence within the various sections of the document and overall EU system.
4. Use cases should be presented in a tabular format to convey the detail of the actions within a flow such that dependencies and preconditions of actions are clearly identified and where necessary, directed to alternate flows or actions.

3 QUESTIONS

The following points represent areas that remain unclear (to this reader in any event) that should be further articulated and/or addressed. Once answered, the quality of experts' comments could be more precise.

Section	Question
General	The solution design does not define the oversight role of the (proposed) governing body or go into any detail of how

	enforcement will be conducted by the agencies across the EU. This is after all the point of the EU System. **How is it envisioned this will be achieved?**
Governance Model	The report does not adequately define or present an architecture in relation to the chosen model (A3 Mixed solution, industry/3 ^{d} party). Who will be the responsible and accountable parties for deciding on how this solution option will be implemented by each Member state (see prior comment on need to further clarify concept of 3 ^{d} party). **Will each Member State decide on the specifics or will this be determined by the manufacturers?**
Page 30: Table 3: Optimal system based on the policy options	The proposed optimal system suggests the *'(S) How - method of adding a security feature'* as the only requirement related to security features. Why was the *'What' – Security features that should be included and/or eligible''* not defined as criteria to the level of detail as in other aspect of the solution design. **It is suggested that the security features be specified in a manner like category (C) Allowed data carriers 'System with limited variety of data carriers for all identification levels and optional data carriers for aggregation packaging levels'.**
4 4.3. Risk Based Surveillance Use Cases	This section is very high-level and does not cater for all of the use cases that are typically involved with investigation and enforcement of illicit trade. For example there is no mention of how an investigative case could be set up based on suspicious activity that the system might detect. Specific emphasis is required to develop the appropriate use cases to support these critical functions. This should include participation from qualified domain experts both internal and external to the EU.
Page 160 onwards, Sections 5.3.1.1 and 5.3.1.2	• Data Archiving – page 163 – how far back before data is archived? • Once data is archived, what is the process to undo or retrieve that data? • Data backups – what is the frequency for ensuring that this is done, and what are the enforcement methods to ensure compliance? • Deletion of data – will this be saved to a backup drive/server/storage facility (because nothing is deleted in IT)? • What types of reports are required and with what stakeholders will these be shared with? • How are reports structured? • Page 160, 'system maintenance' – '*The ID Issuer solution shall provide a user interface to allow the system maintenance*' – what is the structure of this interface, is it synchronous, is there an SLA, i.e. what would the expected maintenance action be? With potentially multiple data storage providers, how will this process be controlled and by whom?

	• Page 160, 'data audit trail' – what is being audited or what is being recorded?
	• Page 160/161, '*The ID Issuer solution shall provide a retention period of at least 10 years after the generation of the serial numbers. Serial numbers related records must be kept accessible during this period.*' – does this impact the archiving timeframe?
	• Sections 5.3.1.1 and 5.3.1.2 speak about functional and technical requirements. How are these different in the context of the document?
	• What is the process for downtime? What is the contingency plan for the system being offline?
	
	Field enforcement:
	
	• Has there been any thought or possible assumption on the number of actual employees that would be engaged in the track and trace solution?
	• No mention is made on the field enforcement processes that form part of the track and trace solution. In particular, the activities related to authentication (of potentially 28 different security feature packages). If this functionality is to be included (as it should), then the following needs to be considered:
	  ○ What types of devices will be provided to the organization(s) and how many?
	  ○ Where devices are used in the field, how will these connect real-time?
	  ○ Since the system will rely extensively on look up tables, will there be an offline function.
	  ○ If not, how will information be recorded for later update, and how will that update occur?
	  ○ How will devices be maintained?
	  ○ Will users be trained on the use of devices? If so, how will this training be conducted?

4 DOCUMENT SPECIFIC COMMENTS

Section	Comment
Page 19: Data Carrier	• The report does not specify the security required for the data carrier. Who will be able to read the data carrier, and how? The questions being, will it be able to be reproduced? Will there be a check digit or some other encryption that would prevent non-authorized users from reading the code?

Page 28: Section 2.2.3. Security Features	• "*Concerning the security features a great deal of research was conducted in the Feasibility Study…However, this analysis was not transposed into the options proposed at the end of the Feasibility which were all based on affixed paper stamps" (pg. 28).* • Taking exception to this statement as it is misleading and leaves the impression that something was unjustifiably omitted during the Feasibility Study. This is not the case, it was the EC's decision to not include any security features that were considered to be "bleeding edge" and not currently employed (at the time of the study) in ANY commercial application of a scale comparable to tobacco. Costing, efficacy and overall proof that these technologies could be employed on the scale required for an EU wide solution was the basis for not including them in any of the four security feature packages. The proprietary technologies and solutions of several companies were omitted based on this criterion. • Furthermore, the TPD uses very specific terminology in terms of method of application. As per Article 16 1. "the security feature shall be irremovably, PRINTED or AFFIXED, indelible…. As set out in this expert's prior comments with respect to the affixing method, the rationale and governance about this decision has been previously set out. • Therefore, for the page 28 2.2.3 to be accurate, it should read that these other methods were disqualified on legal, technical and strategic grounds at the time of the study. A strategic choice has been made to re-visit this based on consultation with the stakeholders. • Several of these technologies appear to now feature to be poised as the foundation of the security features in the EU system. In fact, with the selection of S3- Mixed solution as the optimal policy system, it advocates the selection of any of these solutions. They have been scored very favorably now (highest ranking as per the table on page 301) without any sound justification or reference point other than the "expert knowledge of the contractor and expert subcontractors" (page 301). • Should this type of security feature be chosen by the industry for the EU solution, this lack of referenceable objectivity may be questioned.
Page 37 – Section 4.1.1.3. Cost, effort and funding source	• Figure 5 depicts intra-EU imports as moving from manufacturer to importer to wholesale/distribution. This may be the case; another likely scenario is that the product will move directly from manufacturer to wholesale/distribution or via a warehouse (bonded or otherwise). This is commonly known as drop-shipping were the importer may never actually take physical possession of the goods.

	• The distinction is important and the parties in control of the goods between these steps are different and thus require different types and levels of control. Ultimately, from a governance perspective, who is responsible for ensuring that legitimate marks are placed on all products – manufacturer, importer, government agency? Who will perform this validation and how? If all validation is to occur at manufacture, it implies a production control heavy solution with a strong enforcement capability in country of consumption. If, on the other hand a distributed validation model is adopted (placing responsibility on all entities along the supply chain to ensure validity) then the control can be more evenly spread with less of a reliance on consumer country enforcement.
Page 39 – 4.1.1.5. Scope	• 'Tobacco products produced in the European Union but intended to be exported to non-EU countries do not require a security feature in the terms of article 16 of the TPD.' Does this imply that goods destined for export will not be tracked and traced?
Page 39 – 4.1.1.6. Assumptions	• The assumption states that all EOs and DCOs will adapt their system to meet TPD requirements, but does not state a timeline. Can it be assumed that all EO's and DCO's will need to be ready for implementation by May 2019? Critically, the assumption also does not mention the government agencies that will be required to adapt their systems and processes to be able to manage/oversee/monitor the solution.
Page 39 – 4.1.1.7. Constraints	• The capacity building and enforcement capabilities of government agencies (usually Customs and Excise) needs to be considered as a constraint as well, as it is ambitious to assume that these agencies will be ready within the given timeline. Disconnect between implementation of the solution and enforcement
Page 39 – 4.1.1.8. Roadmap	• Timing seems overly ambitious considering the solution option decision will only be finalized by the end of 2017.
Page 42 – 4.1.2.2. Stakeholders	• Lists the key actors of the tobacco supply chain as manufacturers, Importers and wholesalers/distributors. I would consider the transporters a key actor as well considering they assume responsibility and accountability of the products between the other stakeholders, and are often the source of illicit trade.
Page 48 – 1.1 Generate the serial numbers	• The first step in the process mentions requesting of serial numbers. What criteria will form the basis of this request? Will it be per batch, production run, day, week, quarter, year, etc.? Will it be unique, and identifiable to each manufacturer? Will it require mandatory input parameters for the request?
Page 49 – Activity 1.1.3. Provide the set of serial numbers	• How long will these serial numbers be active? Will they have a "shelf-life" before the manufacturer must make use of them? What happens if they are not used? How will the ID issuer and the surveillance team know that issued serial numbers were never used? Similar to deactivation process described in the document, a proactive process is required to identify serial numbers that are not used by the manufacturer.
Page 52 – 3.2. Report the unique identifiers	• In the process map, the primary data storage is mentioned. Who is the owner and manager of this data store? Who will appoint this entity, the competent authorities or each manufacturer?

Page 54 – 4.1. Generate the serial numbers aggregation	• Will this step be required for each level of aggregation – carton, master case, pallet, etc.? It is unclear whether these will be generated in batch in advance of packing or if it will need to be requested in the process of packing.
Page 62 – Activity 7.1.2. Collect trade information	• This step states 'Before dispatching the aggregation packaging levels, the manufacturers/ importers must collect the trade information, as required by the TPD: - 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.' This assumes that the manufacturer will not be able to sell goods to a distributor without them knowing of the destination of the goods prior to retail. It is stated as required by TPD but doesn't state which section. Regardless, is this practical?
Page 63 – Activity 7.1.5. Block dispatch until acknowledgement is received	• This step seems like an unnecessary delay in the supply chain process. What is the need to wait for acknowledgement of receipt? The communication system should have redundancy built to keep transmitting until the information is received.? What value is acknowledgement providing unless some verification is being provided before responding? If the products are marked incorrectly it will be picked up in dispatch or in the next step.
Page 64 – 8.1. Reception (entry) of the tobacco products and transmission	This process presents a few challenges: • The decision step prior to 9.1, 10.1 and 11.1 is an OR but re-aggregation cannot occur before de-aggregation so there is a step missing or they are not in the correct flow. • The acknowledgement step. Once again, I question the necessity of this step, but in this case, I also question why it occurs prior to validation of the information. Surely, if the receipt information is found to be questionable then those products must be 'stopped' and 'held' at that point and not allowed to continue through the supply chain? Step 8.5 of notifying discrepancies is an after the fact occurrence and will not assist from an enforcement point of view.
Page 69 – 10.1. Generation of the serial numbers for the re-aggregation activities	• Once again, the requesting of serial numbers for aggregation purposes is overkill. See previous point from **page 54.**
Page 80 – 4.3. System users	• There seems to be a dearth of mention of Customs or other enforcement agencies. They are (R)esponsible for enforcing the system and accountable for monitoring the efficacy of the system. This is a major gap in the current solution design.
Page 97: Section 4.5 'System Architecture'	• Who performs the oversight of the implemented solution i.e. who is the owner of the solution/data/etc., or who is information reported to and what is the resultant responsibility of that entity? i.e. who holds overall accountability for the solution? • How, and who will handle the significant integration required for oversight to be performed? In order to enable this integration for oversight and enforcement, has the following been considered?: o An integration standard to govern the integration method between the systems and the protocols used e.g. MQ, web services, FTP, etc.

	○ A specification governing technology that may be used i.e. what are the allowed languages, protocols, the limitations, rules regarding protocols, etc. in order to ensure that technical standards are maintained for integration; ○ The relationships (unique identifiers, etc.) between the systems in terms of data, risk rules and validation, storage repositories, etc.; ○ Any external relationships and dependencies e.g. integration to obtain master data for validation purposes; ○ Who are the relevant third parties or stakeholders, what are their involvements, how are they impacted technically (in order to fully understand this, their systems will need to be understood as well). • Technical, business, functional and test specifications. The business requirements must go into the type of detail that encourages workshops and discussions, analysis, etc. resulting in the various detailed functional, testing and technical specifications.
Page 98, Section 4.5.2 'Architectural Goals'	• The verbal explanations need detailed descriptions and technical backup. The question is, how exactly will each of those goals be met? E.g. extract on Security on page 99 '*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).*' • How will each of these security principle points be enforced?
Page 176 – 5.4.4. Technical requirements	• reference loop in the requirement '- The size and placement of the data carrier must be defined by the requirements presented in section 5.4.4' and 'The printing technique must comply with the quality standards proposed in section 5.4.4'. (same for section 5.5.4)
Page 231 – Section 5.10.4. Proposed Methodology	• The methodology section speaks about the SDLC very briefly and it is standard boilerplate definition. Shouldn't it also mention capacity building in detail (unless of course this would be a separate specification). Capacity building and training could be a challenge considering the timeframe of implementation. With 20 May 2019 as the initial start, to do this effectively, capacity building of the appropriate skills and resources needs significant attention.
Page 231 – Section 5.10.4. Proposed Methodology	• Prior to implementation, the solution would need rigorous testing both for functionality and performance. The charter or plan needs to account for sufficient time to do this, as well as details of how this testing will be done. In addition, the entire T&T process including systems communications, data storage, integrity, regression, as well as the integrity problems (page 216 – 5.9.4.1 Sequence of recovery activities), etc. must be tested.

	• A testing plan and layout should be a section of its own within the document to cater for and detail the test approach of every requirement of the T&T system.
Page 293 – Activity 0.1.2. Integrate the security feature directly on the tobacco product –	• Where are the options of what type of integrated packaging security feature that can be applied? Actual paper manipulation or reading for a digital fingerprint, or printing directly onto the packaging or something else? This would be a critical differentiator if not standardized so I believe it needs to be elaborated on further, or if elaborated further elsewhere, it needs to be referenced.
Page 294 – System users: Governing Body of the T&T system	• Accountable for 'The Governing Body of the Tracking and Tracing System would be accountable for the control of the integration of the security features on the tobacco products taking in consideration the different methods that can be used to proceed with it'. What exactly does 'control of the integration' mean? This statement is too vague for such an integral function.
Page 294 - 295 – System Users and RACI Matrix	• The business process diagram in Activities 0.1.2 and 0.1.3 list 'Member States or an independent third party nominated by the Member States are responsible for the control of the integration of the security features on the tobacco product' and yet these entities are not listed as responsible system users or identified in the RACI matrix.
Page 296 – Security Features	• The extract '*Please note that the list presented below is a non-exhaustive list of potential security features. As there is a constant evolution of new security features, it may by that new features are developed during the course of this current project*' is not a business requirement. It indicates no minimum standard regarding what must be adhered to. Why was no attempt made to classify these security features in terms of their efficacy? Similar to providing a 'limited variety of data carriers' for track and trace purposes, a limited variety of security features should have been defined.
Page 297 – 8.4.1. Technical requirements – Overt components –	• A printed barcode is not a security feature. The text states: 'Barcodes and code verification services are sometimes marketed as an overt (or "digital") security feature. In addition to an overt security feature needing to be 'visible to naked eye' it needs to be discernible as a security feature for it to meet the requirement. A printed barcode does not present the level of uniqueness that the other overt security features provide to make them discernible as such, and therefore should not be included as a security feature. • Furthermore, the admittedly arbitrary table rating on page 301 regarding it being partially tamper-proof. How exactly would a consumer, or enforcement officer for that matter be able to OVERTLY look at a printed bar-code and know whether it has been tampered with or not? An affixed barcode (meaning printed onto another overt form of security feature, with tamper resistant and evident features) could be presented as a viable overt security feature.
Page 301 – Section 8.4.5. Technical requirements – Components compatibility –	• With regard to the availability of credible references regarding the pricing of security features, this is only partially correct. The Feasibility study used a range, there are a few involved in the

	manufacturing and selling of these capabilities, however the prices remain undisclosed. To obtain this, they require direct communication. There is also a site that offers reports of security feature costs in various continents but again these are also obtained via a request and subsequent purchase.
Page 303 8.4.5	• *"It is important to note that 23 out of 28 Member States currently apply fiscal marks in the form of tax stamps."* • It is also important to note as presented in the table that all the 23 countries use the method of affixing. This means that all the production lines used to produce tobacco for these 23 member states are ALREADY fitted with label applicators.
Page 303 – 8.5.1. Operational management requirements –	• This whole section places emphasis on the MS taking accountability for the bulk of the security feature requirements with an after-thought mentioned in the last point regarding ensuring all authorities can read and test such features. • The enforcement effort for such an approach will be tremendous if one assumes that a large volume of the cigarettes produced within the union crosses the border at some time and therefore would need to be assessed by customs agents other than the producing country agents. The approach to allow such flexibility when it comes to the type and level of security feature to be included goes against the fundamental understanding that T&T without security is flawed. At the very least, the report should grade the different types of security features available (beyond the vague and unverifiable table on page 301) in terms of how they meet the requirements of the TPD. If I were a MS reading this report, and when considering which SF, I would implement, it would help if I could see a graded scale of security features from most secure to least secure coupled with their relative cost. This would place me in a much more informed position to decide where on the grading scale I would like (and can afford) to be.
Page 304 – 8.5.2. Size and placement rules –	• this section is presented as *requirements*, but elaborates on size and placement *options* without providing clear guidance on what the preferred or best option may be for each product type. Once again, I feel that not enough attention was paid to understanding the different options which has resulted in vague security feature requirements being defined.
Page 306 – 8.6. Risks and Contingency Plans –	• **T**he mitigation for the second risk 'Security feature not able to be authenticated' provides the controls for authentication, but does not provide mitigation(recovery) action if it cannot be authenticated, as I would assume an SF that cannot be authenticated is not authentic…risk should not be on this list.
Page 306 – 8.6. Risks and Contingency Plans –	• The third risk: 'Production of security features not secure' mentions how the production of the security feature needs to be monitored and audit trailed but it does not mention by whom or how this will be done. I did not see mention of this information being uploaded to, or monitored by the surveillance data so who will be held accountable should the SF production process be compromised? It speaks to the prevailing attitude that comes through in the report that the SF is a support to, and not a fundamental part of the control.

Page 307 – 8.7. Rotation Rules–	• The chapter explains the current MS view on rotational rules and mentions the recommendations made in the feasibility study, but does not attempt to take it further in terms of what options may be available in terms of rotation. An option would be to suggest that during initial design and implementation of the primary SF, a 'secondary' SF should be designed which will stand ready for immediate deployment should the primary SF be compromised. This chapter needs to be analyzed and elaborated further to be of value.
General	• During development of enabling legislation and policy, the EU Commission may consider specifying the required categories of security features using terms aligned to the NASPO and ISO12931:2012(E). It is anticipated that this may aid keeping the EU Commission standards aligned to the intended objectives of the TPD. • Member States may consider the addition of including a forensic security element for the purposes of collecting court-admissible evidence to support investigation and enforcement efforts by Member States.