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 II – Second Draft

EXPERT WORKING GROUP COMMENTS BY [redacted] [redacted]
[redacted]

As discussed during the Expert Workshop, December 14, 2016, Brussels

1 GENERAL COMMENTS

The following general comments are organised by the Alternative Policy Options as contained in the Implementation Analysis. Since they are related to the overall concepts and evaluation of the policy options, they need to be considered in context of the report as a whole. Thus, should they be taken on by the Commission changes would need to be reflected across the various sections of the report (e.g., detailed evaluation, cost benefit analysis etc.).

1.1 GOVERNANCE MODELS (5.4.1)

- 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 time and again to be complicit in the proliferation of illicit trade. In fact, the industry as a whole can be considered serial offenders. Irrespective of the fact that the industry has made considerable efforts to promote itself as one of the key protagonists in the fight against illicit trade, the fact remains that incidents continue to arise (UK, South Africa, Kenya etc.). Thus, the very premise of a 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 incentivised to circumvent controls is bound to fail. As articulated, during the Expert Workshop, the tobacco industry was never intended to be a "partner" with regard to implementation of Article 8 of the Protocol.
- From a governance and technical perspective, the solution should first and foremost be robust enough to prevent manipulation by the industry or other illicit traders as this is the very raison d'etre of the Protocol.
- Further to these points, any solution chosen should be subject to a vulnerability assessment in terms of "how" and "where" vulnerabilities in the system can be exploited. Then, these vulnerabilities and related risks must be addressed with countermeasures which may take the form of business processes, procedures, regulatory oversight, standards or technology components.
- Usage of standards across the various solution elements, where they exist or where they are credibly emerging should be the basis for any relevant element or core function with respect to solution e.g., generation of UID, secure marking, security feature control, data standards, etc.
- Given the reliance on the concept of "3rd party", this needs to be further explored and defined. In the literal sense a 3rd party is simply an unrelated party interacting at "arm's length". I am of the opinion that a 3rd party in terms of the solution must not have had a pre-existing financial or business relationship with the tobacco industry.

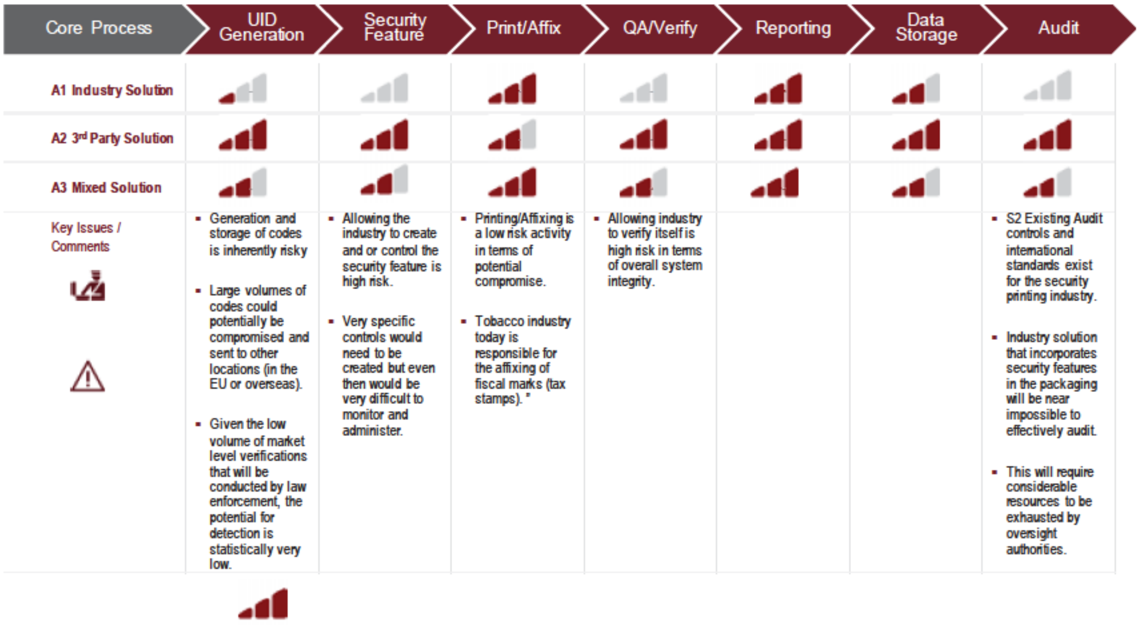
1.1.1 VULNERABILITIES RELATED TO THE THREE GOVERNANCE MODELS

- Of the three governance models proposed, the industry solution (A1) is inherently the highest risk in terms of preventing the industry from circumventing controls as they have historically been known to do (3rd shift production, oversupplying neighbouring markets, etc).
- A system that is put in place and monitored on a day-to-day basis by multiple independent third parties (A2) authorised by the Member States provides the highest degree of control and is least likely to be compromised. Penalties and fines for third parties could also be put in place as an additional regulatory control.

- A mixes system of Governance (A3) could work so long as it is done in a secure manner with the third party being responsible for creation of UIDs and the security features as well as verification of such codes and marks.

- The table below provides a preliminary vulnerability assessment across the core value chain in relation to the three proposed governance models. Please note, that until such time that the detailed solution design is completed, it is not possible to conduct a thorough assessment.

- **This Expert believes that giving the tobacco industry control of the UID and security feature in an environment characterised only by "trust-based", audit controls is tantamount to allowing them to build the perfect "Trojan horse" that can easily be manipulated and be the source of considerable illicit trade under the guise of control.**



Core Process	UID Generation	Security Feature	Print/Affix	QA/Verify	Reporting	Data Storage	Audit
A1 Industry Solution	▮▯▯	▯▯▯	▮▮▮	▯▯▯	▮▮▮	▮▮▯	▯▯▯
A2 3rd Party Solution	▮▮▮	▮▮▮	▮▮▯	▮▮▮	▮▮▮	▮▮▮	▮▮▮
A3 Mixed Solution	▮▮▯	▮▮▯	▮▮▮	▮▮▯	▮▮▮	▮▮▯	▮▮▯
Key Issues / Comments ⚠	▪ Generation and storage of codes is inherently risky ▪ Large volumes of codes could potentially be compromised and sent to other locations (in the EU or overseas). ▪ Given the low volume of market level verifications that will be conducted by law enforcement, the potential for detection is statistically very low.	▪ Allowing the industry to create and or control the security feature is high risk. ▪ Very specific controls would need to be created but even then would be very difficult to monitor and administer.	▪ Printing/Affixing is a low risk activity in terms of potential compromise. ▪ Tobacco industry today is responsible for the affixing of fiscal marks (tax stamps). "	▪ Allowing industry to verify itself is high risk in terms of overall system integrity.			▪ S2 Existing Audit controls and international standards exist for the security printing industry. ▪ Industry solution that incorporates security features in the packaging will be near impossible to effectively audit. ▪ This will require considerable resources to be exhausted by oversight authorities.

▮▮▮

Figure 1 - Preliminary Vulnerability Assessment

1.2 METHODOLOGY AND SCORING OF VARIOUS OPTIONS

- It is challenging to provide meaningful comments with respect to the various options are scored and evaluated. For example, with respect to application of the security features, it would require specific definition of "other method", "mixed method" "integrating" down to the level of the underlying technology. How can it be possible to score and weight and conduct cost benefit analysis with respect to these undefined elements? Nevertheless, the Detailed Analysis of Each Policy Option does so and in many cases the rationale appears to be completely subjective. Indeed, the industry solution and 3rd party solutions are presented as extremes and the undefined solutions ("integrating", "different" "mixed" etc.) are positioned as a compromise position between the two. This needs to be better defined in order to stand up to intense scrutiny that is likely to come from multiple vectors.

1.3 SECURITY FEATURE FEATURES AND METHOD OF APPLICATION (SECTION 4.5)

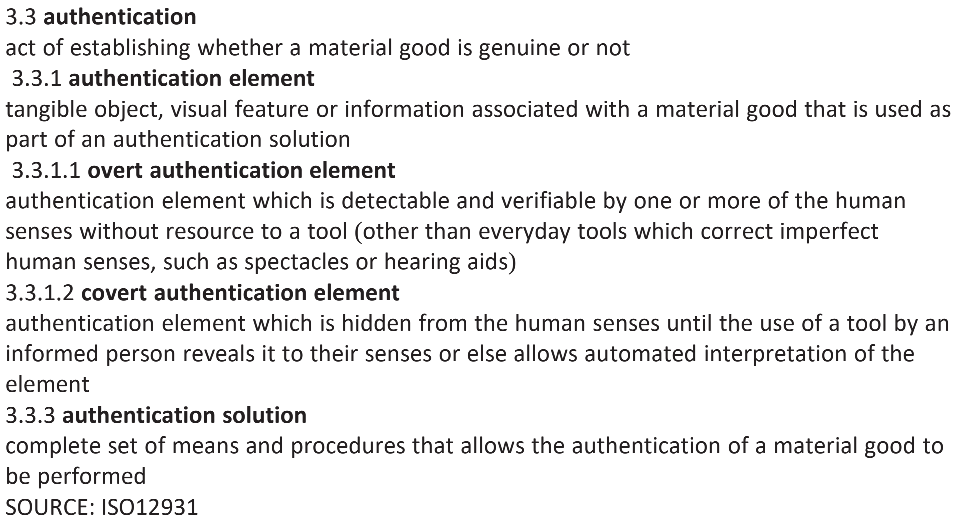
- As discussed at length in the workshop, this section of the report is flawed and incomplete with respect to the rationale used and the overall scoring across the dimensions. Much of the knowledge base established during the Feasibility Study was not carried forward.
- Article 16 of the TPD states the following: “the security feature shall be irremovably, **PRINTED** or **AFFIXED**, indelible and not hidden or interrupted”. The TPD does not mention “other” or “mixed” or integration with packaging or the emerging field of digital fingerprinting. I would suggest a more thorough reading of Section 9.1 of the Feasibility Study with regard to method of application of the security features and the agreed choice by the Commission at the time that “affixed” was the best option.
- 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 first phase of the Feasibility Study involved extensive market research (desk based, survey based, benchmarking and site visits). The analysis team had the task of analysing both publically available information as well as information obtained directly from industry security feature and traceability providers.
- A register of security feature providers was established and cross checked for inclusiveness with relevant trade associations. These were categorised according to the security feature type e.g., “visible”/Overt, “covert”/Invisible and in turn mapped to the Problem Statement (FS 4.2.2.).
- A policy decision/guidance was prompted by the analysis team that across the project, and wherever possible existing generally accepted standards (as recognised by national or international bodies) would be used with respect to the individual solution components. As with the data centric solution elements standards were used as a basis for evaluation of security features and method of affixing. With respect to security features analysis and recommendations were aligned to ISO 12931[1] and others relating in to regulation of security feature providers (e.g., ISO 14298[2], CWA15374[3] NASPO, etc.).

[1] **ISO 12931:2012**: Performance criteria for authentication solutions used to combat counterfeiting of material goods

[2] **ISO 14298 – Management of Security Printing Processes:** For producers of documents of value, e g Banknotes, ID documents or security foils, which are physically protected against counterfeiting by added security features ISO 14298 establishes requirements for the management of security printing processes

[3] **CWA15374 – The certification for suppliers to the Security Printing Industry**: All suppliers of products that include security features or of services that ensure the physical security of printed matter manufactured by a Security Printing Company can be audited against the CWA 15374

- Incorporating the security feature with the commercial packaging or directly printing it onto the packs presents a challenge in terms of controlling the distribution of those features (e.g., commercially available packaging and inks).
- This would also raise concerns about the potential for collusion given the fact that many of the suppliers of such integrated features are also large, long-time commercially connected suppliers to the tobacco industry.
- The following definitions were used with regard security features:



3.3 **authentication**
act of establishing whether a material good is genuine or not
3.3.1 **authentication element**
tangible object, visual feature or information associated with a material good that is used as part of an authentication solution
3.3.1.1 **overt authentication element**
authentication element which is detectable and verifiable by one or more of the human senses without resource to a tool (other than everyday tools which correct imperfect human senses, such as spectacles or hearing aids)
3.3.1.2 **covert authentication element**
authentication element which is hidden from the human senses until the use of a tool by an informed person reveals it to their senses or else allows automated interpretation of the element
3.3.3 **authentication solution**
complete set of means and procedures that allows the authentication of a material good to be performed
SOURCE: ISO12931

- 5 methods of application of the security feature were considered (see below excerpts from the Feasibility Study).

9.1.1 METHOD OF APPLICATION

In addition to the package of security feature elements, a key consideration is the method in which these security features can be applied to each unit of tobacco product. The five methods considered include:

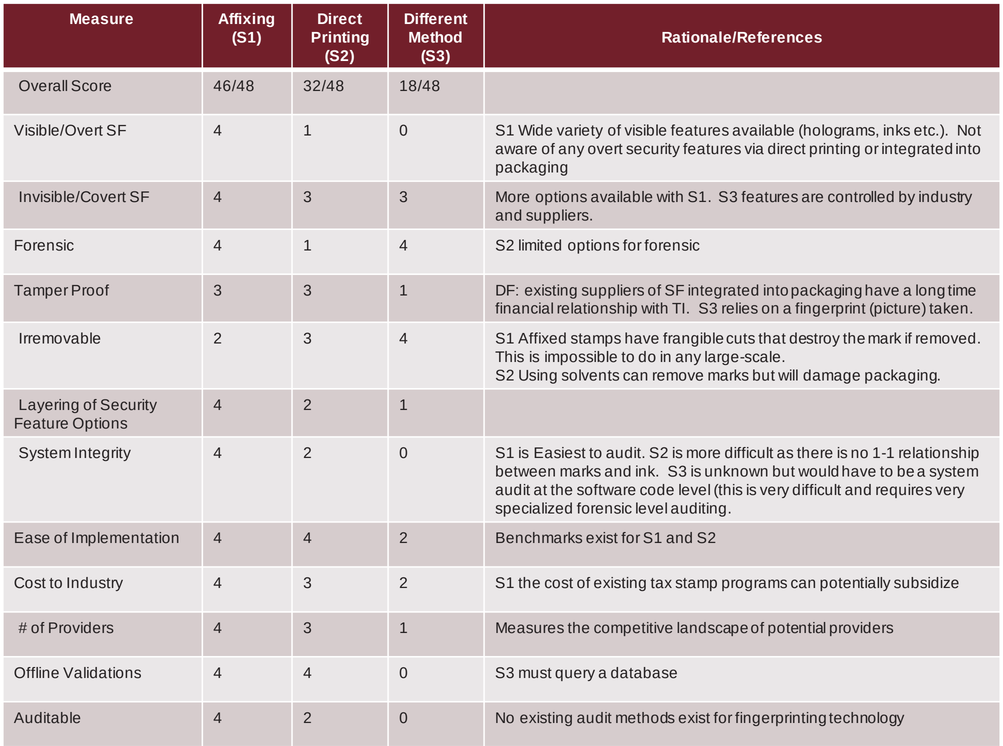
1. *Incorporating the security feature as part of the production of the packaging material itself.*
2. *Including the security feature in a specific element of the packaging that can be controlled (e.g. tear tape).*
3. *Printing the security feature using security inks directly onto the product.*
4. *Providing the security feature as self-contained security package as a label, film or stamp.*
5. *Security feature combined with fingerprinting of unique material properties of the package*

Key advantages of this method:

- *Opportunity to include all four security layers (overt, semi-covert, covert and forensic) to improve security value.*
- *Security printers are used to handle sensitive material like papers, security elements, security inks, semi-finished and finished goods. Certification and compliance requirements require all steps of the production to be documented including material balance, batches, and waste.*
- *Existing secure supply chain logistics are used for both inputs to the security feature, and control of storage and distribution itself.*
- *Flexibility and choice of available security elements that can be used because of control of inputs including security papers, inks and features are available to security printers (some security element providers only allow delivery to certified and security printers).*
- *Similarity to method used for tax stamps means this equipment can be used with existing processes and equipment that can potentially be leveraged.*

- *The control of stamps during manufacturing process is known and generally accepted. Provides accurate volume verification (important for reconciling integrity of the overall tobacco traceability solution discussed in Section 8.6.1.2.*
- *The application of stamps is possible for full scope of manufacturing processes: automated and high volume production lines, imported goods can be labelled at the manufacturing site abroad and low volume production lines can be labelled manually.*

- The figure below displays a ranking table for the different methods related to the choice of security features. It is based on the research conducted during the feasibility study as well as relevant benchmarks and site visits to numerous tobacco and excise goods manufacturing facilities. It also includes research from other related projects. It does not take into consideration stakeholder survey's or marketing communications as they are inherently biased on all sides. It is, however, subjective based on the expertise of the author.



Measure	Affixing (S1)	Direct Printing (S2)	Different Method (S3)	Rationale/References
Overall Score	46/48	32/48	18/48	
Visible/Overt SF	4	1	0	S1 Wide variety of visible features available (holograms, inks etc.). Not aware of any overt security features via direct printing or integrated into packaging
Invisible/Covert SF	4	3	3	More options available with S1. S3 features are controlled by industry and suppliers.
Forensic	4	1	4	S2 limited options for forensic
Tamper Proof	3	3	1	DF: existing suppliers of SF integrated into packaging have a long time financial relationship with TI. S3 relies on a fingerprint (picture) taken.
Irremovable	2	3	4	S1 Affixed stamps have frangible cuts that destroy the mark if removed. This is impossible to do in any large-scale. S2 Using solvents can remove marks but will damage packaging.
Layering of Security Feature Options	4	2	1	
System Integrity	4	2	0	S1 is Easiest to audit. S2 is more difficult as there is no 1-1 relationship between marks and ink. S3 is unknown but would have to be a system audit at the software code level (this is very difficult and requires very specialized forensic level auditing.
Ease of Implementation	4	4	2	Benchmarks exist for S1 and S2
Cost to Industry	4	3	2	S1 the cost of existing tax stamp programs can potentially subsidize
# of Providers	4	3	1	Measures the competitive landscape of potential providers
Offline Validations	4	4	0	S3 must query a database
Auditable	4	2	0	No existing audit methods exist for fingerprinting technology

Figure 2 - Method of Security Feature Application

1.4 . UNIQUE IDENTIFIER (UID)

- **Under any of the Governance models proposed, the UID must be generated independently of the tobacco industry in a secure environment where the codes cannot be copied**. Given the low potential for large amounts of codes to be checked once on the market, coupled with the fact that tobacco products are fast moving consumer goods, which do not stay in circulation very long, it is highly possible that there could be large numbers of duplicate codes (which have been somehow compromised) put onto legitimate or counterfeit packs without ever being detected. A statistical analysis of this was done by SBS as an informal work paper and revealed the near impossibility of detection given the overall market size of the EU.

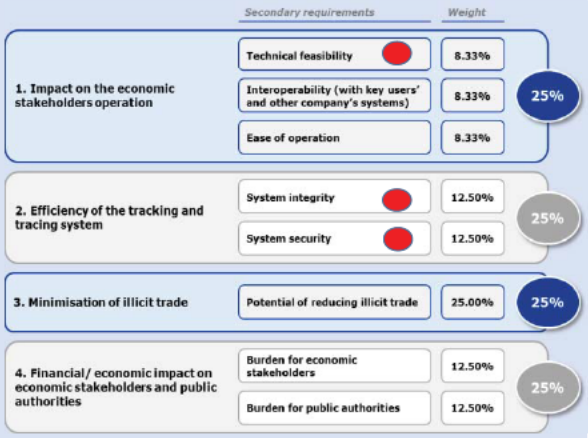
- Thus, the code generator should be independent of Tobacco Industry systems and within the control of the Competent Authority either directly or indirectly via a 3rd party. This will also affect the scoring of Section 4.1 related to the Governance Models.
- The Unique Identifier should also be quality assured and verified prior to being added to the data-base and aggregation levels applied. This also should be conducted by an independent 3rd party to address potential vulnerabilities that are inherent in the manufacturing environment (e.g., duplicated codes).

1.5 DATA STORAGE

- The analysis around data storage models is logical and forms the basis for policy decisions related to the next step. I Agree with the outcome of the analysis: Combined Model is optimal.
- It is a bit pre-mature to analyse the performance of the various data storage models without first defining the specific use cases based on each stakeholder that will need to query the database(s). The commission may also wish to consider reviewing typical use cases based on the most common types of fraud topologies experienced by the EU (see Section 2.3/Figure 13 of FS).

2 SPECIFIC COMMENTS

The following comments pertain to specific sections in the report as noted in the Reference.

<table>
<tr><th>Reference</th><th>Comment</th><th>Recommendation</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>**P 27, S 2.3.1.2 Selection Criteria**</td><td>
Secondary requirements | Weight
1. Impact on the economic stakeholders operation — 25%
Technical feasibility ● | 8.33%
Interoperability (with key users' and other company's systems) | 8.33%
Ease of operation | 8.33%
2. Efficiency of the tracking and tracing system — 25%
System integrity ● | 12.50%
System security ● | 12.50%
3. Minimisation of illicit trade — 25%
Potential of reducing illicit trade | 25.00%
4. Financial/ economic impact on economic stakeholders and public authorities — 25%
Burden for economic stakeholders | 12.50%
Burden for public authorities | 12.50%

Not all criteria can be treated equally in terms of the overall objectives of the TPD and Protocol. Some might be considered absolutes, without which there is no point for the solution. Others are "nice to haves", whereby the main intent of the of the system can be realised without the being in place.

Technical feasibility, system integrity, system security, Potential for reducing illicit trade should be weighted absolutely.</td><td>- Establish two-tier ranking system. "**Absolutes**", which require a minimum level of performance and others which can be weighted and scored.
- Alternatively, increase the weight of item 2.</td></tr>
<tr><td>**P 24, S2.2.4**</td><td>*"Regarding tracking and tracing, no option covers completely all the requirements for the implementation of Article 15 of the TPD…."*

First, in working closely with the EC, it was agreed that all four options were compliant with TPD and Protocol. The only outstanding question was whether the industry solution as featured in Option 1 and 3 would meet the Article 8 (12) provisions of the Protocol.

The Implementation Analysis does NOT provide an explanation as to what extent the four options proposed in the Feasibility Study were not compliant with Article 15? It simply states this as a fact without attribution.

The notion that only the industry can capture Article 15 data elements (a-k) is false. Indeed, the industry has proven, in its own solution, Codentify that it is technically feasible to capture much of this information</td><td>Edit IA to reflect accurately the findings and recommendations of the Feasibility Study.</td></tr>
</table>

	already. Either in its own systems or with collaboration between supply chain partners. This could also be achieved across all the Options proposed via integration with tobacco industry systems.	
P 24, S2.2.4	*"Concerning the security features, a great deal of research was conducted on the Feasibility Study, which contains, generically, all the options for security features currently available on the market. However, this analysis was not transposed into the options proposed, which are all based on an affixed paper stamp."* Given the nature of the research (desk and survey based) it was not possible to validate that all of the technologies and solutions existed in the real world. Indeed, some were found to be entirely conceptual or lab based (e.g., technology or solution physically existed but was not actually implemented anywhere). With regard to certain methods of security features, it was agreed with the Commission that only those features that could be demonstrated in an actual "real world" implementation would be included as an option. Additional criteria that went into consideration were as follows: • Cost of security features; • Variety of security features available for each layer of security (visible, invisible, etc.); • Proven efficacy and robustness of security features; • Existing systems in place in the tobacco domain (e.g., tax stamps); and, • Number of suppliers that could potentially provide security features. Since multiple references and related actual implementations meeting the above criteria we identified, and a robust and highly competitive (non-proprietary) market for such	

	features existed vis-à-vis "affixed paper stamps" the method of affixing for all four options was chosen as the lowest risk for all parties. It was noted that there was a category of "emerging" security features but that there was not enough evidence of their commercial usage (efficacy, cost etc.) in any pertinent benchmarks and not at all in the tobacco domain (see FS Section 4.2).	
P 37, S3.1	*Regarding the allocation of responsibilities and functions, the TPD already defines the individual stakeholders which are responsible for several processes of the system. On the other hand, it is possible to isolate and identify other functions, actions and processes which may be considered integral to the functioning of the system, but for which the TPD and the FCTC Protocol do not assign a clear responsible. These may include:* • *The responsibility for **generation of the unique identifier** for each unit packet of tobacco products.* • *The printing or affixing of the unique identifier on the tobacco unit packs.* • *The **verification of the unique identifier**.* *While the TPD and the FCTC Protocol do not explicitly mention the above actions, there are some considerations that need to be taken into account when allocating responsibility for them to the different actors involved in the process. Recital 31 of the TPD indicates the general requirement for the design of the tracking and tracing system, which is the need to ensure its independence and transparency. Another consideration is related to the concept of 'control'*[4][5] *of the full system, as required by the FCTC Protocol. It **is important to highlight that 'control' does not necessarily mean 'ownership' of the***	This section, in defining the industry operated solution establishes a view that rather should be considered from a legal (and not speculative) perspective. "control does not mean ownership" is purely speculative. Article 8(12) clearly states "conditions assigned to the party shall not be **performed by** or **delegated to** the tobacco industry".

[4] Art. 8.2 FCTC Protocol: *"Each Party shall establish, in accordance with this Article, a tracking and tracing system, controlled by the Party for all tobacco products that are manufactured in or imported onto its territory taking into account their own national or regional specific needs and available best practice."*

[5] Art.8.12 FCTC Protocol: *"Obligations assigned to a Party shall not be performed by or delegated to the tobacco industry."*

	system. *The final configuration must allow the competent authorities to control (supervise and direct the actions or function of) the system, while other actors (industry or third party) may be those actually operating/performing some of the activities needed.*	
Pg 78/9 S3.5	*"This combination of security elements can generate a stronger security feature, as for someone to engage in illicit trade of tobacco products it would be necessary to circumvent all security elements implemented".* This statement is unqualified. In fact, it must be considered that security features generated from material properties inherent in the packaging (e.g., fingerprinting) are less secure given the fact that there is no direct count of them (e.g. generating them from fibres in paper). They are also not created in controlled facilities (as is the case with other security features). Security features generated from physical or materials means (holograms, inks etc.) can be audited and be measured in terms volumes of raw materials (which are also subject to stringent controls as opposed to those materials used by commercial printers). Since the fingerprints are generated from the packaging itself, the only limit of them is the availability of the packaging materials. This is not suitable for products that are highly susceptible to illicit trade. If this option is to be allowed, considerable controls will be required to be established.	
Pg 122, S4.5.2.4	The analysis favours "printing or Integrating" or "Any Method" but without being very specific about what these mean. How can one rate these according to the criteria. E.g., with regard to system integrity, both of these score the highest whilst Affixing scores the lowest. With regard to "affixing" one can get an independent count of the number of marks (stamps) created, one knows that they only come from controlled sources (security printers) who are often government bodies themselves or closely linked to (and therefore	Re-visit analysis and rankings.

	have a lot to lose) governments. This rating therefore appears arbitrary.	
P123, S4.5.2.6	*"Given the risks presented before, options '(S2) Printing or integrating through a different method' or '(S3) Any method' are considered to have a perfect score on the 'Potential to reduce illicit trade'. This is not true, however, for option '(S1) Affixing'."*	Unqualified statement with no basis in fact or evidence.
P 196/7, S7.5General: Security Feature Combined with Fiscal Mark (Tax Stamp) 197 S1	78% (22 of 28) Member States have fiscal marks, many of which have security feature configurations already in line with Article 16 (or relatively close to it), to establish a security feature standard with some mandatory and some optional features would preserve market competitiveness, but also provide a modicum of standardisation (e.g., allow flexibility in Overt and semi-overt via OVI, Holograms etc., but proscribe the use of the same forensic marks across the Member States.	Adopt a standard-based approach to the security feature options and ensure multiple independent providers can supply them.
FS 9.1.1.4 PROVIDING THE SECURITY FEATURE AS A LABEL OR STAMP	Key advantages of this method: - Opportunity to include all four security layers (overt, semi-covert, covert and forensic) to improve security value. - Security printers are used to handle sensitive material like papers, security elements, security inks, semi-finished and finished goods. Certification and compliance requirements require all steps of the production to be documented including material balance, batches, and waste. - Existing secure supply chain logistics are used for both inputs to the security feature, and control of storage and distribution itself. - Flexibility and choice of available security elements that can be used because of control of inputs including security papers, inks and features are available to security printers (some security element providers only allow delivery to certified and security printers).	

	- Similarity to method used for tax stamps means this equipment can be used with existing processes and equipment that can potentially be leveraged. - The control of stamps during manufacturing process is known and generally accepted. Provides accurate volume verification (important for reconciling integrity of the overall tobacco traceability solution). - The application of stamps is possible for full scope of manufacturing processes: automated and high volume production lines, imported goods can be labelled at the manufacturing site abroad and low volume production lines can be labelled manually.	
Pg 122, S4.5.2.4	With regard to system integrity S2 and S3 score the highest whilst Affixing scores the lowest. We know that with regard to "affixing" we can get an independent count of the number of marks (stamps) created, we know that they only come from controlled sources (security printers) who are often government bodies themselves or closely linked to governments (and therefore have a lot to lose). Based on research related to S2 from the Feasibility Study, the tobacco industry has lined up existing long-time suppliers who currently provide security features for the tobacco industry's own business purposes (namely anti-counterfeiting) to somehow qualify under the Protocol and TPD. It must be noted that the security feature package and related traceability suggested in the Protocol and TPD is there to prevent large-scale release of "genuine" illicit product on the market.	
9.1.1.6METHOD OF APPLICATION USED FOR THIS ASSESSMENT	The secure label / stamp provided additional implementation flexibility, choice of security elements and compatibility with both high speed and low volume tobacco production volume over direct marking.	Note rationale
7.5 S3 "Any Method"	All 28 member states could conceivably choose its own method. This could make the monitoring of security features, particularly those related to direct printing or integrated into packaging nearly impossible to enforce/monitor.	

	section 9.1 of the Feasibility Report assessed different affixing options - with advantages and disadvantage of each. The Implementation Analysis does not respond in any meaningful way to how the disadvantages will now be overcome going for a “any method” approach.	
P 199:	*“For the products in which the security feature is printed or integrated through a different method, the method of application itself guarantees that it remains tamper proof and irremovable”.* *When the security feature is affixed, although this is, in principle, more vulnerable, there are also ways to make it completely tamper proof and irremovable.”* This contradicts the ranking it was accorded.	This is unqualified. “Different method” what does this entail? How can one impose a modicum of control when the method has not been defined? These methods are also “bleeding edge”.
199 1-1	Disagree with ranking given fact that nearly 80% of MS already have affixed tax stamps. Thus, that means that 80% of the production lines for EU are already fitted with label applicators. Security features to comply to the yet to be defined EU standard would need to be added, but this happens with the respective security printer. How can “any method” rate higher when we don’t know what it is, is not in practice in the market today?	Cost benefit analysis should be amended to reflect this.
P 203 4.1:	S1 related to risks associated with paper based stamps, this view clearly originates from the industry, highly secure stamps that require on-line activation are nearly impossible to be copied. Counterfeiting of “old school” stamps is indeed a problem, particularly in developing countries where the stamps are not secure and are not combined with robust material-based and digital security features. It is very easy to copy a “simple” “dumb” stamp, but even a stolen secure stamp would not be activated during the production process and therefore would be detectable during the authentication process.	