Targeted stakeholder consultation on the implementation of an EU system for traceability and security features pursuant to Articles 15 and 16 of the Tobacco Products Directive 2014/40/EU

Fields marked with * are mandatory.

This is a targeted stakeholder consultation. The purpose of this consultation is to seek comments from stakeholders:

- directly affected by the upcoming implementation of an EU system for traceability and security features pursuant to Articles 15 and 16 of the new Tobacco Products Directive (Directive 2014/40/EU), or
- considering to have special expertise in the relevant areas.

In the Commission's assessment, the following stakeholders, including their respective associations, are expected to be directly affected:

1. manufacturers of finished tobacco products,
2. wholesalers and distributors of finished tobacco products,
3. providers of solutions for operating traceability and security features systems,
4. governmental and non-governmental organisations active in the area of tobacco control and fight against illicit trade.

Not directly affected are retailers and upstream suppliers of tobacco manufacturers (except the solution providers mentioned in point 3 above).

The basis for the consultation is the Final Report to the European Commission's Consumers, Health and Food Executive Agency (CHAFEA) in response to tender n° EAHC/2013/Health/11 concerning the provision of an analysis and feasibility assessment regarding EU systems for tracking and tracing of tobacco products and for security features (hereafter the Feasibility Study). The Feasibility Study was published on 7 May 2015 and is available at http://ec.europa.eu/health/tobacco/docs/2015_tpd_tracking_tracing_frep_en.pdf. The interested stakeholders are advised to review the Feasibility Study before responding to this consultation.

The comments received in the course of this consultation will be an input to the further implementation work on a future EU system for traceability and security features. In particular, the comments will be taken into account in a follow-up study.

Stakeholders are invited to submit their comments on this consultation at the following web-address https://ec.europa.eu/eusurvey/runner/trace until 31 July 2015. The web-based survey consists of closed and open questions. For open questions stakeholders will be asked to provide comments up to the limit of characters indicated in the question or to upload (a) separate document(s) in PDF format up to the limit of total number of standard A4 pages (an average of 400 words per page) indicated in the question. Submissions should be - where possible - in English. For a corporate group one single reply should be prepared. For responses from governmental organisations, which are not representing a national position, it should be explained why the responding body is directly affected by the envisaged measures.

The information received will be treated in accordance with Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community (please consult the privacy statement). Participants in the consultation are asked not to upload personal data of individuals.

The replies to the consultation will be published on the Commission's website. In this light no confidential information should be provided. If there is a need to provide certain information on a confidential basis, contact should be made with the Commission at the following email address: SANTE-D4-SOHO-and-TOBACCO-CONTROL@ec.europa.eu with a reference in the email title: "Confidential information concerning targeted stakeholder consultation on the implementation of an EU system for traceability and security features". A meaningful non-confidential version of the confidential information should be submitted at the web-address.

Answers that do not comply with the specifications cannot be considered.

A. Respondent details

*A.1. Stakeholder's main activity:

- a) Manufacturer of tobacco products destined for consumers (finished tobacco products)
- b) Operator involved in the supply chain of finished tobacco products (excluding retail)
- c) Provider of solutions
- d) Governmental organisation
- e) NGO
- f) Other

*A.1.c. Please specify:

- i) Provider of solutions for tracking and tracing systems (or parts thereof)
- ii) Provider of solutions for security features (or parts thereof)
- iii) Data Management Providers (or parts thereof)

*A.2. Contact details (organisation's name, address, email, telephone number, if applicable name of the ultimate parent company or organisation) - if possible, please do not include personal data

Text of 1 to 800 characters will be accepted

Worldline NV
Haachtsesteenweg 1442
1130 Brussels - Belgium
Tel: +32 2 7276111
Parent Company:
Atos
River OUEST 80, Quai Voltaire
95877 Bezons - France

*A.3. Please indicate if your organisation is registered in the Transparency Register of the European Commission (unless 1d):

(•) Yes ( ) No

*A.3.1. Please enter your registration number in the Transparency Register

249876817241-03

*A.4. Extract from the trade or other relevant registry confirming the activity listed under 1 and where necessary an English translation thereof.

- **297043ab-1645-4d98-ba1c-d1e4fc895490/Extract Worldline Registry.pdf**

B. Options proposed in the Feasibility Study

B.1. Please rate the appropriateness of each option for tracking and tracing system set out in the Feasibility Study in terms of the criteria listed in the tables below

B.1.1. Option 1: an industry-operated solution, with direct marking on the production lines carried out by tobacco manufacturers (for further details on this option, please consult section 8.2 of the Feasibility Study)

	Appropriate	Somewhat appropriate	Neutral	Somewhat inappropriate	Inappropriate	No opinion
*Technical feasibility	◉	○	○	○	○	○
*Interoperability	◉	○	○	○	○	○
*Ease of operation for users	◉	○	○	○	○	○
*System integrity (e.g. low risk of manipulation)	○	◉	○	○	○	○
*Potential of reducing illicit trade	◉	○	○	○	○	○
* Administrative/financial burden for economic operators	◉	○	○	○	○	○
* Administrative/financial burden for public authorities	◉	○	○	○	○	○

B.1.2. Option 2: a third party operated solution, with direct marking on the production lines carried out by a solution or service provider (for further details on this option, please consult section 8.3 of the Feasibility Study)

	Appropriate	Somewhat appropriate	Neutral	Somewhat inappropriate	Inappropriate	No opinion
*Technical feasibility	○	○	○	◉	○	○
*Interoperability	○	○	◉	○	○	○
*Ease of operation for users	○	○	○	◉	○	○
*System integrity (e.g. low risk of manipulation)	○	○	○	◉	○	○
*Potential of reducing illicit trade	○	○	○	◉	○	○
* Administrative/financial burden for economic operators	○	○	◉	○	○	○
* Administrative/financial burden for public authorities	○	○	◉	○	○	○

B.1.3. Option 3: each Member State decides between Option 1 and 2 as to an entity responsible for direct marking (manufacture or third party) (for further details on this option, please consult section 8.4 of the Feasibility Study)

	Appropriate	Somewhat appropriate	Neutral	Somewhat inappropriate	Inappropriate	No opinion
*Technical feasibility	○	○	◉	○	○	○
*Interoperability	○	○	○	○	◉	○
*Ease of operation for users	○	○	○	○	◉	○
*System integrity (e.g. low risk of manipulation)	○	○	◉	○	○	○
*Potential of reducing illicit trade	○	○	○	○	◉	○
* Administrative/financial burden for economic operators	○	○	○	○	◉	○
* Administrative/financial burden for public authorities	○	○	○	○	◉	○

B.1.4. Option 4: a unique identifier is integrated into the security feature and affixed in the same production process (for further details on this option, please consult section 8.5 of the Feasibility Study)

	Appropriate	Somewhat appropriate	Neutral	Somewhat inappropriate	Inappropriate	No opinion
*Technical feasibility	○	○	○	○	◉	○
*Interoperability	○	○	○	○	◉	○
*Ease of operation for users	○	○	○	○	◉	○
*System integrity (e.g. low risk of manipulation)	○	○	○	◉	○	○
*Potential of reducing illicit trade	○	○	○	○	◉	○
* Administrative/financial burden for economic operators	○	○	○	○	◉	○
* Administrative/financial burden for public authorities	○	○	○	○	◉	○

B.1.5. Please upload any additional comments on the options referred to in question B.1 (max. 5 pages)

- **3e78b353-b67f-4f1f-8cac-c4b8bcc89b18/EC Consultation_additional answers from Atos.pdf**

B.2. Please rate the appropriateness of each option for security features set out in the Feasibility Study in terms of the criteria listed in the tables below

B.2.1. Option 1: a security feature using authentication technologies similar to a modern tax stamp
(for further details on this option, please consult section 9.2 of the Feasibility Study)

	Appropriate	Somewhat appropriate	Neutral	Somewhat inappropriate	Inappropriate	No opinion
*Technical feasibility	○	○	○	○	◉	○
*Interoperability	○	○	○	○	◉	○
*Ease of operation for users	○	○	○	◉	○	○
*System integrity (e.g. low risk of manipulation)	○	○	○	○	◉	○
*Potential of reducing illicit trade	○	○	○	○	◉	○
* Administrative/financial burden for economic operators	○	○	○	○	◉	○
* Administrative/financial burden for public authorities	○	○	○	◉	○	○

B.2.2. Option 2: reduced semi-covert elements as compared to Option 1 (for further details on this option, please consult section 9.3 of the Feasibility Study)

	Appropriate	Somewhat appropriate	Neutral	Somewhat inappropriate	Inappropriate	No opinion
*Technical feasibility	○	○	○	◉	○	○
*Interoperability	○	○	○	○	◉	○
*Ease of operation for users	○	○	○	◉	○	○
*System integrity (e.g. low risk of manipulation)	○	○	○	○	◉	○
*Potential of reducing illicit trade	○	○	○	◉	○	○
* Administrative/financial burden for economic operators	○	○	○	○	◉	○
* Administrative/financial burden for public authorities	○	○	○	○	◉	○

B.2.3. Option 3: the fingerprinting technology is used for the semi-covert and covert levels of protection (for further details on this option, please consult section 9.4 of the Feasibility Study)

	Appropriate	Somewhat appropriate	Neutral	Somewhat inappropriate	Inappropriate	No opinion
*Technical feasibility	○	○	○	◉	○	○
*Interoperability	○	○	○	◉	○	○
*Ease of operation for users	○	○	○	◉	○	○
*System integrity (e.g. low risk of manipulation)	○	○	○	◉	○	○
*Potential of reducing illicit trade	○	○	○	◉	○	○
* Administrative/financial burden for economic operators	○	○	○	◉	○	○
* Administrative/financial burden for public authorities	○	○	○	◉	○	○

B.2.4. Option 4: security feature is integrated with unique identifier (see Option 4 for traceability)
(for further details on this option, please consult section 9.5 of the Feasibility Study)

	Appropriate	Somewhat appropriate	Neutral	Somewhat inappropriate	Inappropriate	No opinion
*Technical feasibility	○	◉	○	○	○	○
*Interoperability	○	◉	○	○	○	○
*Ease of operation for users	○	○	○	◉	○	○
*System integrity (e.g. low risk of manipulation)	○	○	○	○	◉	○
*Potential of reducing illicit trade	○	○	○	○	◉	○
* Administrative/financial burden for economic operators	○	○	○	○	◉	○
* Administrative/financial burden for public authorities	○	○	○	◉	○	○

B.2.5. Please upload any additional comments on the options referred to in question B.2 (max. 5 pages)

C. Cost-benefit analysis

C.1. Do you agree with?

	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	No opinion
*The benefit analysis presented in section 11.3.1 of the Feasibility Study	○	○	○	◉	○	○
*The cost analysis presented in section 11.3.2 of the Feasibility Study	○	○	○	○	◉	○

*C.1.1. If you selected option "Disagree" or "Somewhat disagree" in the previous question, please upload your main reasons for disagreement (max. 5 pages)

- **c8862a27-a82b-4163-8658-13cecdadc1ba/EC Consultation_additional answers from Atos.pdf**

D. Additional questions

The questions in this section relate to different possible building blocks and modalities of the envisaged system (questions D.1, D.3, D.4, D.6, D.8, D.10, D.12, D.14 and D.16). When replying please take into account the overall appropriateness of individual solutions in terms of the criteria of technical feasibility, interoperability, ease of operation, system integrity, potential of reducing illicit trade, administrative/financial burden for economic stakeholders and administrative/financial burden for public authorities.

*D.1. Regarding the generation of a serialized unique identifier (for definition of a unique identifier, see Glossary in the Feasibility Study), which of the following solutions do you consider as appropriate (multiple answers possible)?

- [x] a) A single standard provided by a relevant standardization body
- [ ] b) A public accreditation or similar system based on the minimum technical and interoperability requirements that allow for the parallel use of several standards;
- [ ] c) Another solution
- [ ] d) No opinion

*D.1.a. Please indicate your preferred standardization body

Text of 1 to 400 characters will be accepted

We recommend GS1 or similar industry coding standard.
GS1 standards are already implemented and used by the vast majority of operators in the FMCG supply chain and in the tobacco products supply chain.
Most of the IT companies have practical experience with GS1 Standards.

D.2. Please upload any additional comments relating to the rules for generation of a serialized unique identifier referred to in question D.1. above (max. 2 pages)

*D.3. Regarding (a) data carrier(s) for a serialized unique identifier, which of the following solutions do you consider as appropriate (multiple answers possible)?

- [x] a) Solution based on a single data carrier (e.g. 1D or 2D data carriers)
- [ ] b) Solution based on the minimum technical requirements that allow for the use of multiple data carriers;
- [ ] c) Another solution;
- [ ] d) No opinion

*D.3.a. Please indicate your preferred data carrier and explain why

Text of 1 to 400 characters will be accepted

We suggest the use of 2D data carriers. It enables to handle the required information within the limited available space on the pack. For lowest level packaging, dot code supports machine readable and human readable codes at high speeds.
We do not recommend the use of QR codes (due to its lengthy coding and decoding delay), nor 1D barcodes (requires more space on the pack than available).

*D.4. Regarding (a) data carrier(s) for a serialized unique identifier, which of the following solutions do you consider as appropriate (multiple answers possible)?

- [ ] a) System only operating with machine readable codes;
- [x] b) System operating both with machine and human readable codes;
- [ ] c) No opinion

D.5. Please upload any additional comments relating to the options for (a) data carrier(s) for a serialized unique identifier referred to in questions D.3 and D.4 above (max. 2 pages)

- **68539cf2-28ad-4378-bbd3-c069d098d00b/EC Consultation_additional answers from Atos.pdf**

*D.6. Regarding the physical placement of a serialized unique identifier, when should it happen (multiple answers possible)?

- [ ] a) Before a pack/tin/pouch/item is folded/assembled and filled with products;
- [x] b) After a pack/tin/pouch/item is folded/assembled and filled with products;
- [ ] c) No opinion

D.7. Please upload any additional comments relating to the placement of a serialized unique identifier referred to in question D.6. above (max. 2 pages)

D.8. Which entity should be responsible for?

	Economic operator involved in the tobacco trade without specific supervision	Economic operator involved in the tobacco trade supervised by the third party auditor	Economic operator involved in the tobacco trade supervised by the authorities	Independent third party	No opinion
*Generating serialized unique identifiers	○	○	◉	○	○
*Marking products with serialized unique identifiers on the production line	○	○	◉	○	○
*Verifying if products are properly marked on the production line	○	◉	○	○	○
*Scanning products upon dispatch from manufacturer's/importer's warehouse	○	◉	○	○	○
*Scanning products upon receipt at distributor's/wholesaler's premises	○	◉	○	○	○

*Scanning products upon dispatch from distributor's/wholesaler's premises	○	◉	○	○	○
*Aggregation of products	○	◉	○	○	○

D.9. In relation to question D.8. above, please specify any other measures that your organisation considers relevant

Text of 1 to 1200 characters will be accepted

> An industry implemented and operated solution, based upon government prescribed standards and specifications, which are validated and audited by a third party (for example Data Management Provider), will ensure a practical, secure and cost efficient setup.

*D.10. Regarding the method of putting the security feature on the pack/tin/pouch/item, which of the following solutions do you consider as appropriate (multiple answers possible)?

- [ ] a) A security feature is affixed;
- [ ] b) A security feature is affixed and integrated with the tax stamps or national identification marks;
- [x] c) A security feature is printed;
- [x] d) A security feature is put on the pack/tin/puch/item through a different method;
- [ ] e) No opinion

*D.10.d. Please explain your other method

Text of 1 to 800 characters will be accepted

> For secuity purposes we recommend a direct print onto the pack, as opposed to gluing or affixing. This will prevent that the security feature can be easily copied or stolen for usage on counterfeit packs.

D.11. Please upload any additional comments relating to the method of putting the security feature on the pack referred to in question D.10 above (max. 2 pages)

- **e3bf52fb-bcf4-43a3-8704-4e6d15e6f06b/EC Consultation_additional answers from Atos.pdf**

*D.12. Regarding the independent data storage as envisaged in Article 15(8) of the TPD, which of the following solutions do you consider as appropriate (multiple answers possible)?

- [x] a) A single centralised storage for all operators;
- [x] b) An accreditation or similar system for multiple interoperable storages (e.g. organised per manufacturer or territory);
- [ ] c) Another solution
- [ ] d) No opinion

D.13. Please upload any additional comments relating to the independent data storage referred to in question D.12. above (max. 2 pages)

- **97257af9-117a-4dcb-b4d0-9eaf5d10b7e3/EC Consultation_additional answers from Atos.pdf**

*D.14. In your opinion which entity(ies) is/are well placed to develop reporting and query tools (multiple answers possible)?

- [x] a) Provider of solutions to collect the data from the manufacturing and distribution chain;
- [x] b) Provider of data storage services;
- [ ] c) Another entity
- [ ] d) No opinion

D.15. Please upload any additional comments relating to the development of reporting and query tools referred to in question D.14. above (max. 2 pages)

- **cd8bfb36-fe6d-4e0b-a5d8-e57fed7381a0/EC Consultation_additional answers from Atos.pdf**

*D.16. Do you consider that the overall integrity of a system for tracking and tracing would be improved if individual consumers were empowered to decode and verify a serialized unique identifier with mobile devices (e.g. smartphones)?

- (•) a) Yes
- ( ) b) No
- ( ) c) No opinion

D.16.a. If yes, please explain your considerations

Text of 1 to 800 characters will be accepted

More verifications, for example by involving citizens, will ultimately lead to better insights about illicit trade. The information which they collect can be an extra source for analytical tools capable of providing new insights into the phenomenon of illicit trade. We refer to our response to D15 for further background.

D.17. Please upload any additional comments on the subject of this consultation (max. 10 pages)

- **c72a728a-5184-4907-b49d-0090045c3477/EC Consultation_additional answers from Atos.pdf**

Contact

✉ SANTE-D4-SOHO-and-TOBACCO-CONTROL@ec.europa.eu

Attachment A4

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
	[redacted]
	[redacted]
	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

EC Consultation – Atos written statements

Atos SE (Societas Europaea) is a leader in digital services with 2014 pro forma annual revenue of circa € 11 billion and 93,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. A trusted partner for governmental institutions in many European countries, Atos provide services in areas such as e-tax filing, defence/ intelligence/ security systems, electronic truck tolling, as well as intelligent electronic regulatory reporting systems.

Atos has set up a Global Centre of Competence Serialization that supports the local application of IT systems to effectively fight illicit trade. Through the Centre we have successfully implemented effective, IT based Product Authentication and Track & Trace solutions across several industries, from pharmaceutical to tobacco and luxury goods.

B.1.5.

Option 1: Option 1 provides several advantages compared to the other options. It is based on an outlined cooperation between the authorities and the private sector. Compared to the other options it allows for capturing industry key learnings and leveraging the existing methods and installed systems. The option is based on reusing the existing systems currently used by the industry. This increases feasibility and cost efficiency for all stakeholders. It also reduces system implementation lead time.
We see two key benefits of an outlined cooperation with the tobacco industry:

- Many different companies already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats.

That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.
The Atos Competence Centre was involved in relevant Authentication and Track & Trace projects in different industries, including tobacco, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.
It is imperative Option 1 is implemented and operated under stringent control and audit rules as defined and endorsed by the Authorities.

Option 2: While Option 2 could leverage the advantages related to an EU wide approach (i.e. leading to one harmonized system), we foresee serious issues with the technical and organizational feasibility of this scenario.
Given the EU market size of tobacco products and the related amount of events to be captured, the size and manageability of one EU data repository would be very challenging. Also the alignment of the member states is a complicating factor. We fear this will result in delays in implementation time and will

not lead to a user friendly system, with compromises on usability (ex. system response time) and functionality.
The suggestion in Section 8.3.1 'Key principles' to replicate data to the Member States will increase overall level of efforts, both for the involved Solution Providers and the Member States, and lead to a higher overall cost.
Section 8.3.1'Key principles' also states that the solution may be operated by one (or more) solution provider(s) implementing a community wide traceability system. It is likely this would in fact create a kind of monopoly position for this solution provider. The European and National authorities would become dependent on one single solution provider. This can have negative impact on the cost efficiency and will limit the dynamics of future innovation.
Option 2 therefor does not seem to be a very realistic scenario, as the alignment of all Member States and stakeholders will be challenging due to mentioned technical, economical, but also organizational inconveniences.

Option 3: This option would increase costs unnecessarily (cost of dbase replication), prevent economies of scale and is not a good basis for encouraging collaboration between Member States, which is a prime condition for effectively fighting illicit trade. Since the databases would be driven by the Member States, the exchange of information and view on the complete supply chain is becoming difficult. Moreover, it goes against the reality of illicit trade, which is for the largest part organized internationally, and is currently exploiting the inability of Member States to collaborate. It would also create substantial challenges for the manufacturers, who would need to abide several Member State defined solutions, with each solution potentially operated by a different solution provider. The chance is very likely that this Option will not achieve what it is supposed to be doing: reduce illicit trade.

Option 4:
In general terms we support the search for creating synergies by means of combining the traceability option with the security feature based upon integrating the Unique Identifier. A key condition to creating such a synergy is to opt for security features based on digital technologies.
Since all 4 suggested Options related to security features involve a paper based stamp in some format, this does not seem feasible: combining a 'digital' data carrier with a paper based security features will not lead to synergies. It will complicate matters, and create extra costs without providing value.
This Option demonstrates the main issue of how the study has been handled: It wrongly assumes that the only viable security features available today are 'traditional' technologies linked to paper stamps or banderoles. The study did not properly investigate the potential of digital alternatives. New technologies such as digital tax stamps or fingerprinting technology can provide a lot of advantages over paper based technologies.
Moreover, there is a lot of focus on the security features itself and less on the practicality of the proposed paper based security systems, which is a missed opportunity. Digital alternatives will support the activities from the stakeholders* fighting illicit trade a lot better, and will allow for better integration with T&T systems (*Customs, Tax Authorities, Border police, Criminal Police,…).
If not reevaluated, it will cause the current Option 4 to fail its purpose and not lead to the economies as described in Section 8.5 of the feasibility study.

B.2.5.

As a general comment we disagree with the report and analysis, which only focuses on traditional solutions, while not exploring innovative and new solutions. The potential benefits of technologies such

as digital stamps, fingerprint of the products pack or fingerprint of the authorized printers should have been analyzed in the report.
Instead, the report only focused on exploring security features based on paper-based stamps or labels, and suggesting in all 4 options that paper stamps are needed. These are often counterfeited and create a false sense of security, as it may only provide information about the label itself, not the product. The ambition of TPD, and what it is trying to achieve, requires the use of advanced technologies which enable the authentication of products based on the individual physical properties of the product. A key success factor will be the ability to provide authentication of the pack, not a stamp or a label. It is therefore important that the Commission orients itself to embracing and promoting new technologies.

C.1.1.

The feasibility study has only focused on assessing traditional 'paper based' security feature technologies. As referred to in Section 8.5.1 'Key Principles' of Tobacco Traceability Option 4, this is the key building block you could integrate with the 'digital' traceability solution to explore synergies. We refer to our relevant remarks under Section 4 in B.1.5 of this document, in which we state that the combination of a 'digital' data carrier with a paper based security features will not lead to synergies. We therefor suggest that 'digital' alternatives are properly evaluated in a follow up study.
The study fails to reflect on the practicality of the different Options, and how some of the key stakeholders* would benefit from the systems, or not (*Customs, Tax Authorities, Border police, Criminal Police who focus on fighting illicit trade). We are convinced that in case new technologies would have been considered, the benefit analysis would be substantially better. The current benefit analysis as described in Section 11.3 is simply generic and fails to provide tangible value to the Commission and the EU MS.
We agree with the finding of the report under Section 11.3.1 'Benefit Analysis' that it is likely that any combination of the 4 solution options will provide 'similar' results. We think however this result will be mediocre to poor in case new technologies are not adequately considered. We think this would be a missed opportunity. For example: the described 'traditional' tax stamps and overt security features have been around for many years but have not proved very successful for goods identification and fighting illicit trade. They are found to be copied easily, or removed from a legal pack to be used on smuggled products or counterfeited. The ambition of this feasibility study could have been to look for systems which could really make a difference, by using new technologies which are often already in use by different industries.
Furthermore the analysis misses out on assessing the potential impact of enhancing public awareness and actively engaging EU citizens, better field inspection methodologies and control, and the impact of strengthened law enforcement. How will the described Options either help or not in these areas?
Modern technology solutions could help combat counterfeiting and illicit trade. It requires the EU to go beyond what most Member States have been doing until now, and suggest the way forward is to evaluate the available new technologies. We therefore believe this study is a missed opportunity.
For example, taggant technology systems have a low implementation cost since it is integrated into the pack, while it reduces the risk for counterfeiting and fraud. Certain manufacturers and distributors have already installed this technology and are using it, providing potential economies of reusing this existing system. This has unfortunately not been considered in the analysis.

The costs related to Option 4 under 11.2.3 seem underestimated: based on the relevant experience of Atos syncing 2 separate solutions (one for printing and one for verifying) will lead to substantially higher implementing and operating costs.
Based on conversations with different Member States, we see as well that the Total Cost Of Ownership (TCO) linked to the use of tax stamps is generally underestimated (cost of transportation and storage, risk management of counterfeit,…)
Given the missed opportunity for studying the above described benefits, the costs and calculations as presented in 11.3.2 may be academic but bear limited value. We do not have insight on the modeling techniques and assumptions which have been mentioned under Section 11. Without this info it is not possible to provide further comments on Section 11.3.2.

D.2.

We recommend the use of GTIN and serial number as the unique code for the individual product/SKU level, and SGTIN for other packaging levels. For generation of a serialized Unique Identifier, we recommend a highly secure algorithm which takes into consideration the manufacturer, the individual product (SKU), based on a high level of randomization.

D.5.

We believe both machine and human readable codes are required:
A human readable code allows for every consumer to be involved in the process of verifying the authenticity of the product. It can also serve as a backup solution in case the machine readable code can't be read.
A machine readable code will help authorities to efficiently perform verifications. A machine readable code is essential during the manufacturing process, as a human readable code would not be able to support the printing at production speeds. A machine readable code is equally suited to support the aggregation process, which is at the heart of any effective track and trace offering. Machine readable codes could also be used by consumers with a smartphone, eliminating the risk of misreading the human readable code. A Covert Machine readable code also allows to include more information in the coding.

D.11.

We refer to our earlier remark that the feasibility study is only focused on assessing traditional 'paper based' security feature technologies. The report fails to assess alternative methods such as tear tape embedded with security features (which is used in many countries to carry covert, overt and forensic authentication technologies). Main advantage of this type of security feature is that it becomes an integral part of the existing packaging specification. This would reduce the impact and costs in terms of additional infrastructure requirements, and would be an alternative to the costly paper tax stamps, which are known to be easily copied or stolen.

D.13.

Based on the experience and expertise from Atos in the domain of Data management and storage, and reflecting on the requirements as described in Article 15 (8) of TPD, we point out the following important pillars related to Integration services & IT Security:

Integration services

To ensure an easy integration with the external world, the usage of proven market standards is for the envisaged system is important:

- Products are identified by an electronic Product Code (EPC)
- the specification EPCIS (Electronic Product Code Services Information Services) aiming to enable disparate applications to leverage Electronic Product Code (EPC) data via EPC-related data sharing, both within and across (enterprise and government) systems
- pack related information is stored in a machine readable code

From a technological point of view, the solution should be based on Service-Oriented Architecture concepts and provide external interfaces using well-accepted standards (Web Services, WSDL, SOAP) and wide-spread protocols (FTP, HTTP, HTTPS).

IT security : Measures to protect the system and its connections against threats from outside

Due to the amount and sensitivity of the manufacturing data, the system will have a special need for data protection and protection of the system itself, requiring the Data Management Provider to have an ample expertise in planning, implementing and operating security-critical systems.

In order to design an optimized protection the following activities typically need to be performed:

1. Analysis of protection requirement* with regard to the targets of confidentiality, integrity and availability
2. Implementation of an ISMS (Information Security Management System)
3. Implementation of the actual security systems (see listings below)

Step 1 will ensure that we plan for the necessary protection levels and do not overprotect certain areas while neglecting others. Results from the analysis will determine the implementation steps 2 and 3.

Step 2: The Information Security Management System (ISMS) describes all procedures and rules to control, maintain and improve IT-Security. It is absolutely crucial to maintain a consistent protection against the different types of threats. A proven and audited standard ISMS is vital, based upon which extensions and changes to this Standard would have to be implemented.

Step 3: The Technical Security Systems will enforce security rules and enable the automated detection of deviations. For the envisaged system in scope we consider the following security systems to be indispensable:

- Firewall/Proxy Services
- IAM – Identity and Access Management
- IDS/IPS – Intrusion Detection/Prevention System
- Full and strong Data Encryption for all data in transfer outside the datacenter
- Vulnerability Management Services
- Physical high security measures (Atos datacenter standard)

Additional technical systems/measures will be considered depending on the outcome of the protection requirements*:

- Web Application Firewall
- Data Encryption for data in storage, e.g. in the database
- Full and strong Data Encryption for data in transfer inside the datacenter
- DLP – Data Loss Prevention
- SIEM - Security Information and Event Management

- Security Operations Center to handle events from DLP and SIEM
- Strong Authentication by hardware-based digital certificates

In the design and the implementation of such Security Systems, we recommend to follow the relevant standards and all legal regulations (e.g. ISO 2700x). Moreover it is self-evident that in the course of the operations the security system will be audited internally and externally.

IT security : Measures to achieve a strict separation of access to the data of different stakeholders

The ISMS and its technical measures also ensure the high protection levels within the system. Requirements for a strict separation of access to data from the manufacturers will be ensured by employing the following measures:

- Design Measures (the design of the system will enforce that accidental or intentional access violations either from stakeholders or privileged users cannot take place)
    1. Incorporating a robust cloud security assessment service into the analysis of the protection requirements
    2. Designing and implementing an Identity and Access Management
    3. Application architecture supporting multi-tenancy
    4. The business logic has to be built to support multi-tenancy
    5. Physical separation of the databases
    6. Data encryption services inside the data center
- Operations Measures (detecting deviations during operations)
    1. DLP -Data Loss Prevention
    2. SIEM -Security Information and Event Management
    3. SOC - Security Operations Center

D.15.

Both a) and b) could provide reporting and query tools. The provider of data storage services could perform the role of certified interface to the Member States authorities and serve as trusted entity, independent from the manufacturers.

We consider the development of reporting and query tools to be a key consideration for making the TPD a success. It is important to develop and provide to the relevant authorities and stakeholders a highly secured Analysis platform, delivering Preventive IT Systems. This platform would provide advanced analytical capabilities, like anomaly detection, predictive analytics and advanced pattern recognition and would be supported by experts with in-depth vertical domain know-how, paired with advanced analytics skills.

Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective.
This platform would be based on handling different types of information flows consisting of structured and unstructured data, which will, by means of data mining and analytics, lead to useful information.
The main benefits and outcome would be useful information to be used by the relevant authorities for

- ► Spotting and predicting illicit trade patterns
- ► Focusing on critical cases and “big fishes”
- ► Improving efficiency and effectiveness for Law Enforcement

► Improving collaboration with other entities

D.17.

Any proposed tracking and tracing solution for the TPD must have at its heart the ability to uniquely identify products. Unique identification is not only important for the product authentication purposes, but should also support an aggregation process, and build a relationship between different levels of packaging, which is already part of the traditional manufacturing practice.
Interoperability is another key feature. There is a wide choice of existing coding systems suppliers which are supporting manufacturers across the EU and globally, allowing for reuse of the equipment at line level and systems as a whole at governmental or factory level. It is therefore recommended that any adopted tracking and tracing solution for use with the TPD would facilitate the reuse, if compliant with Open Standards.
Allowing as many suppliers as possible to support manufacturers and governments is the only practical approach to gain a successful outcome.
The main items to effectively fight illicit trade: Collaboration between industries and organizations, sharing knowledge and leveraging best practices, promoting open standards and technical development, and leverage the use of new technologies.

The key considerations regarding the implementation of the Tobacco Products Directive from Atos are:

1. **Technology should be part of a broader strategy.** Track &Trace systems can assist authorities to fight the growing issue of illicit tobacco trade. Today's technologies provide substantial improvement opportunities, but should be part of a broader strategy that also includes other measures: effective cross-border data exchange, interactive inspections, intelligent analysis tools, and enforcement in the field.
   Conclusion: technology should be embedded in a broader strategy

2. **International co-operation and information exchange.** Illicit trade is a cross-border phenomenon. The TPD can only be effectively implemented if member states and their enforcement agencies can co-operate and exchange information. The technological consequence of the need for co-operation and exchange is the choice for open standards-based systems. Atos supports the use of GS1 standards to identify products, capture the information at key points in the supply chain and then share the information seamlessly among stakeholders. This approach will ensure:
   - Easy integration with and interoperability between existing governmental systems, enforcement agencies and even industry
   - The ability to work cross border and effectively fight illicit trade
   - Ability of governments to use standard smart-phones and scanning devices for in-field inspections. This reduces cost and complexity, and ensures easy system maintenance.
   - Dependence on one specific supplier or use of proprietary systems will not lead to cost and system efficiency, and will limit future innovation
   - Avoid a European patchwork of standards that will raise the cost and complexity and making an effective tobacco control impossible

   Conclusion: open standards-based systems allow international co-operation and information exchange.

3. **Co-operation with private sector.** We see two benefits of a basic co-operation between the authorities and the private sector, in relation to the implementation of the TPD.

- Many major tobacco suppliers already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats. That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.

The Atos Competence Centre was involved in relevant Authentication and Track &Trace projects, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.

Conclusion: A basic co-operation with affected industries allows government agencies, when implementing the TPD, to benefit from industry's systems, expertise and budgets.

4. **Preventive/ predictive systems** Combining repressive measures and preventive measures is highly effective. Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective. Preventive/predictive systems can be a key tool for different agencies involved in fighting back against illicit trade.
   Important structured data sources are:
   - Digital Track & Trace systems from product suppliers and/or governments: If such systems apply digital coding on the products on the level of the SSU (smallest sellable unit), they can gain a deep insight in the movements of legal and illegal goods in a country.
   - Consumers: Today's smartphone and App technology allow citizens to check the authenticity of a product they are about to purchase. Involving citizens will multiply the amount of data that can be fed into analytical systems.

   Technological conditions for such citizen involvement: digital coding of products on pack level, and the use open standards (Atos supports the use of GS-1 standards)

   Conclusion: the use of preventive/predictive analytical IT systems is highly effective to fight illicit trade, and should be stimulated.

Attachment C.1.1

EC Consultation – Atos written statements

Atos SE (Societas Europaea) is a leader in digital services with 2014 pro forma annual revenue of circa € 11 billion and 93,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. A trusted partner for governmental institutions in many European countries, Atos provide services in areas such as e-tax filing, defence/ intelligence/ security systems, electronic truck tolling, as well as intelligent electronic regulatory reporting systems.

Atos has set up a Global Centre of Competence Serialization that supports the local application of IT systems to effectively fight illicit trade. Through the Centre we have successfully implemented effective, IT based Product Authentication and Track & Trace solutions across several industries, from pharmaceutical to tobacco and luxury goods.

B.1.5.

Option 1: Option 1 provides several advantages compared to the other options. It is based on an outlined cooperation between the authorities and the private sector. Compared to the other options it allows for capturing industry key learnings and leveraging the existing methods and installed systems. The option is based on reusing the existing systems currently used by the industry. This increases feasibility and cost efficiency for all stakeholders. It also reduces system implementation lead time.
We see two key benefits of an outlined cooperation with the tobacco industry:

- Many different companies already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats.

That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.
The Atos Competence Centre was involved in relevant Authentication and Track & Trace projects in different industries, including tobacco, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.
It is imperative Option 1 is implemented and operated under stringent control and audit rules as defined and endorsed by the Authorities.

Option 2: While Option 2 could leverage the advantages related to an EU wide approach (i.e. leading to one harmonized system), we foresee serious issues with the technical and organizational feasibility of this scenario.
Given the EU market size of tobacco products and the related amount of events to be captured, the size and manageability of one EU data repository would be very challenging. Also the alignment of the member states is a complicating factor. We fear this will result in delays in implementation time and will

not lead to a user friendly system, with compromises on usability (ex. system response time) and functionality.
The suggestion in Section 8.3.1 'Key principles' to replicate data to the Member States will increase overall level of efforts, both for the involved Solution Providers and the Member States, and lead to a higher overall cost.
Section 8.3.1'Key principles' also states that the solution may be operated by one (or more) solution provider(s) implementing a community wide traceability system. It is likely this would in fact create a kind of monopoly position for this solution provider. The European and National authorities would become dependent on one single solution provider. This can have negative impact on the cost efficiency and will limit the dynamics of future innovation.
Option 2 therefor does not seem to be a very realistic scenario, as the alignment of all Member States and stakeholders will be challenging due to mentioned technical, economical, but also organizational inconveniences.

Option 3: This option would increase costs unnecessarily (cost of dbase replication), prevent economies of scale and is not a good basis for encouraging collaboration between Member States, which is a prime condition for effectively fighting illicit trade. Since the databases would be driven by the Member States, the exchange of information and view on the complete supply chain is becoming difficult. Moreover, it goes against the reality of illicit trade, which is for the largest part organized internationally, and is currently exploiting the inability of Member States to collaborate. It would also create substantial challenges for the manufacturers, who would need to abide several Member State defined solutions, with each solution potentially operated by a different solution provider. The chance is very likely that this Option will not achieve what it is supposed to be doing: reduce illicit trade.

Option 4:
In general terms we support the search for creating synergies by means of combining the traceability option with the security feature based upon integrating the Unique Identifier. A key condition to creating such a synergy is to opt for security features based on digital technologies.
Since all 4 suggested Options related to security features involve a paper based stamp in some format, this does not seem feasible: combining a 'digital' data carrier with a paper based security features will not lead to synergies. It will complicate matters, and create extra costs without providing value.
This Option demonstrates the main issue of how the study has been handled: It wrongly assumes that the only viable security features available today are 'traditional' technologies linked to paper stamps or banderoles. The study did not properly investigate the potential of digital alternatives. New technologies such as digital tax stamps or fingerprinting technology can provide a lot of advantages over paper based technologies.
Moreover, there is a lot of focus on the security features itself and less on the practicality of the proposed paper based security systems, which is a missed opportunity. Digital alternatives will support the activities from the stakeholders* fighting illicit trade a lot better, and will allow for better integration with T&T systems (*Customs, Tax Authorities, Border police, Criminal Police,…).
If not reevaluated, it will cause the current Option 4 to fail its purpose and not lead to the economies as described in Section 8.5 of the feasibility study.

B.2.5.

As a general comment we disagree with the report and analysis, which only focuses on traditional solutions, while not exploring innovative and new solutions. The potential benefits of technologies such

as digital stamps, fingerprint of the products pack or fingerprint of the authorized printers should have been analyzed in the report.
Instead, the report only focused on exploring security features based on paper-based stamps or labels, and suggesting in all 4 options that paper stamps are needed. These are often counterfeited and create a false sense of security, as it may only provide information about the label itself, not the product. The ambition of TPD, and what it is trying to achieve, requires the use of advanced technologies which enable the authentication of products based on the individual physical properties of the product. A key success factor will be the ability to provide authentication of the pack, not a stamp or a label. It is therefore important that the Commission orients itself to embracing and promoting new technologies.

C.1.1.

The feasibility study has only focused on assessing traditional 'paper based' security feature technologies. As referred to in Section 8.5.1 'Key Principles' of Tobacco Traceability Option 4, this is the key building block you could integrate with the 'digital' traceability solution to explore synergies. We refer to our relevant remarks under Section 4 in B.1.5 of this document, in which we state that the combination of a 'digital' data carrier with a paper based security features will not lead to synergies. We therefor suggest that 'digital' alternatives are properly evaluated in a follow up study.
The study fails to reflect on the practicality of the different Options, and how some of the key stakeholders* would benefit from the systems, or not (*Customs, Tax Authorities, Border police, Criminal Police who focus on fighting illicit trade). We are convinced that in case new technologies would have been considered, the benefit analysis would be substantially better. The current benefit analysis as described in Section 11.3 is simply generic and fails to provide tangible value to the Commission and the EU MS.
We agree with the finding of the report under Section 11.3.1 'Benefit Analysis' that it is likely that any combination of the 4 solution options will provide 'similar' results. We think however this result will be mediocre to poor in case new technologies are not adequately considered. We think this would be a missed opportunity. For example: the described 'traditional' tax stamps and overt security features have been around for many years but have not proved very successful for goods identification and fighting illicit trade. They are found to be copied easily, or removed from a legal pack to be used on smuggled products or counterfeited. The ambition of this feasibility study could have been to look for systems which could really make a difference, by using new technologies which are often already in use by different industries.
Furthermore the analysis misses out on assessing the potential impact of enhancing public awareness and actively engaging EU citizens, better field inspection methodologies and control, and the impact of strengthened law enforcement. How will the described Options either help or not in these areas?
Modern technology solutions could help combat counterfeiting and illicit trade. It requires the EU to go beyond what most Member States have been doing until now, and suggest the way forward is to evaluate the available new technologies. We therefore believe this study is a missed opportunity.
For example, taggant technology systems have a low implementation cost since it is integrated into the pack, while it reduces the risk for counterfeiting and fraud. Certain manufacturers and distributors have already installed this technology and are using it, providing potential economies of reusing this existing system. This has unfortunately not been considered in the analysis.

The costs related to Option 4 under 11.2.3 seem underestimated: based on the relevant experience of Atos syncing 2 separate solutions (one for printing and one for verifying) will lead to substantially higher implementing and operating costs.
Based on conversations with different Member States, we see as well that the Total Cost Of Ownership (TCO) linked to the use of tax stamps is generally underestimated (cost of transportation and storage, risk management of counterfeit,…)
Given the missed opportunity for studying the above described benefits, the costs and calculations as presented in 11.3.2 may be academic but bear limited value. We do not have insight on the modeling techniques and assumptions which have been mentioned under Section 11. Without this info it is not possible to provide further comments on Section 11.3.2.

D.2.

We recommend the use of GTIN and serial number as the unique code for the individual product/SKU level, and SGTIN for other packaging levels. For generation of a serialized Unique Identifier, we recommend a highly secure algorithm which takes into consideration the manufacturer, the individual product (SKU), based on a high level of randomization.

D.5.

We believe both machine and human readable codes are required:
A human readable code allows for every consumer to be involved in the process of verifying the authenticity of the product. It can also serve as a backup solution in case the machine readable code can't be read.
A machine readable code will help authorities to efficiently perform verifications. A machine readable code is essential during the manufacturing process, as a human readable code would not be able to support the printing at production speeds. A machine readable code is equally suited to support the aggregation process, which is at the heart of any effective track and trace offering. Machine readable codes could also be used by consumers with a smartphone, eliminating the risk of misreading the human readable code. A Covert Machine readable code also allows to include more information in the coding.

D.11.

We refer to our earlier remark that the feasibility study is only focused on assessing traditional 'paper based' security feature technologies. The report fails to assess alternative methods such as tear tape embedded with security features (which is used in many countries to carry covert, overt and forensic authentication technologies). Main advantage of this type of security feature is that it becomes an integral part of the existing packaging specification. This would reduce the impact and costs in terms of additional infrastructure requirements, and would be an alternative to the costly paper tax stamps, which are known to be easily copied or stolen.

D.13.

Based on the experience and expertise from Atos in the domain of Data management and storage, and reflecting on the requirements as described in Article 15 (8) of TPD, we point out the following important pillars related to Integration services & IT Security:

Integration services

To ensure an easy integration with the external world, the usage of proven market standards is for the envisaged system is important:

- Products are identified by an electronic Product Code (EPC)
- the specification EPCIS (Electronic Product Code Services Information Services) aiming to enable disparate applications to leverage Electronic Product Code (EPC) data via EPC-related data sharing, both within and across (enterprise and government) systems
- pack related information is stored in a machine readable code

From a technological point of view, the solution should be based on Service-Oriented Architecture concepts and provide external interfaces using well-accepted standards (Web Services, WSDL, SOAP) and wide-spread protocols (FTP, HTTP, HTTPS).

IT security : Measures to protect the system and its connections against threats from outside

Due to the amount and sensitivity of the manufacturing data, the system will have a special need for data protection and protection of the system itself, requiring the Data Management Provider to have an ample expertise in planning, implementing and operating security-critical systems.

In order to design an optimized protection the following activities typically need to be performed:

1. Analysis of protection requirement* with regard to the targets of confidentiality, integrity and availability
2. Implementation of an ISMS (Information Security Management System)
3. Implementation of the actual security systems (see listings below)

Step 1 will ensure that we plan for the necessary protection levels and do not overprotect certain areas while neglecting others. Results from the analysis will determine the implementation steps 2 and 3.

Step 2: The Information Security Management System (ISMS) describes all procedures and rules to control, maintain and improve IT-Security. It is absolutely crucial to maintain a consistent protection against the different types of threats. A proven and audited standard ISMS is vital, based upon which extensions and changes to this Standard would have to be implemented.

Step 3: The Technical Security Systems will enforce security rules and enable the automated detection of deviations. For the envisaged system in scope we consider the following security systems to be indispensable:

- Firewall/Proxy Services
- IAM – Identity and Access Management
- IDS/IPS – Intrusion Detection/Prevention System
- Full and strong Data Encryption for all data in transfer outside the datacenter
- Vulnerability Management Services
- Physical high security measures (Atos datacenter standard)

Additional technical systems/measures will be considered depending on the outcome of the protection requirements*:

- Web Application Firewall
- Data Encryption for data in storage, e.g. in the database
- Full and strong Data Encryption for data in transfer inside the datacenter
- DLP – Data Loss Prevention
- SIEM - Security Information and Event Management

- Security Operations Center to handle events from DLP and SIEM
- Strong Authentication by hardware-based digital certificates

In the design and the implementation of such Security Systems, we recommend to follow the relevant standards and all legal regulations (e.g. ISO 2700x). Moreover it is self-evident that in the course of the operations the security system will be audited internally and externally.

IT security : Measures to achieve a strict separation of access to the data of different stakeholders

The ISMS and its technical measures also ensure the high protection levels within the system. Requirements for a strict separation of access to data from the manufacturers will be ensured by employing the following measures:

- Design Measures (the design of the system will enforce that accidental or intentional access violations either from stakeholders or privileged users cannot take place)
    1. Incorporating a robust cloud security assessment service into the analysis of the protection requirements
    2. Designing and implementing an Identity and Access Management
    3. Application architecture supporting multi-tenancy
    4. The business logic has to be built to support multi-tenancy
    5. Physical separation of the databases
    6. Data encryption services inside the data center
- Operations Measures (detecting deviations during operations)
    1. DLP -Data Loss Prevention
    2. SIEM -Security Information and Event Management
    3. SOC - Security Operations Center

D.15.

Both a) and b) could provide reporting and query tools. The provider of data storage services could perform the role of certified interface to the Member States authorities and serve as trusted entity, independent from the manufacturers.

We consider the development of reporting and query tools to be a key consideration for making the TPD a success. It is important to develop and provide to the relevant authorities and stakeholders a highly secured Analysis platform, delivering Preventive IT Systems. This platform would provide advanced analytical capabilities, like anomaly detection, predictive analytics and advanced pattern recognition and would be supported by experts with in-depth vertical domain know-how, paired with advanced analytics skills.

Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective.
This platform would be based on handling different types of information flows consisting of structured and unstructured data, which will, by means of data mining and analytics, lead to useful information.
The main benefits and outcome would be useful information to be used by the relevant authorities for

- ► Spotting and predicting illicit trade patterns
- ► Focusing on critical cases and “big fishes”
- ► Improving efficiency and effectiveness for Law Enforcement

► Improving collaboration with other entities

D.17.

Any proposed tracking and tracing solution for the TPD must have at its heart the ability to uniquely identify products. Unique identification is not only important for the product authentication purposes, but should also support an aggregation process, and build a relationship between different levels of packaging, which is already part of the traditional manufacturing practice.
Interoperability is another key feature. There is a wide choice of existing coding systems suppliers which are supporting manufacturers across the EU and globally, allowing for reuse of the equipment at line level and systems as a whole at governmental or factory level. It is therefore recommended that any adopted tracking and tracing solution for use with the TPD would facilitate the reuse, if compliant with Open Standards.
Allowing as many suppliers as possible to support manufacturers and governments is the only practical approach to gain a successful outcome.
The main items to effectively fight illicit trade: Collaboration between industries and organizations, sharing knowledge and leveraging best practices, promoting open standards and technical development, and leverage the use of new technologies.

The key considerations regarding the implementation of the Tobacco Products Directive from Atos are:

1. **Technology should be part of a broader strategy.** Track &Trace systems can assist authorities to fight the growing issue of illicit tobacco trade. Today's technologies provide substantial improvement opportunities, but should be part of a broader strategy that also includes other measures: effective cross-border data exchange, interactive inspections, intelligent analysis tools, and enforcement in the field.
   Conclusion: technology should be embedded in a broader strategy

2. **International co-operation and information exchange.** Illicit trade is a cross-border phenomenon. The TPD can only be effectively implemented if member states and their enforcement agencies can co-operate and exchange information. The technological consequence of the need for co-operation and exchange is the choice for open standards-based systems. Atos supports the use of GS1 standards to identify products, capture the information at key points in the supply chain and then share the information seamlessly among stakeholders. This approach will ensure:
   - Easy integration with and interoperability between existing governmental systems, enforcement agencies and even industry
   - The ability to work cross border and effectively fight illicit trade
   - Ability of governments to use standard smart-phones and scanning devices for in-field inspections. This reduces cost and complexity, and ensures easy system maintenance.
   - Dependence on one specific supplier or use of proprietary systems will not lead to cost and system efficiency, and will limit future innovation
   - Avoid a European patchwork of standards that will raise the cost and complexity and making an effective tobacco control impossible

   Conclusion: open standards-based systems allow international co-operation and information exchange.

3. **Co-operation with private sector.** We see two benefits of a basic co-operation between the authorities and the private sector, in relation to the implementation of the TPD.

- Many major tobacco suppliers already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats. That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.

The Atos Competence Centre was involved in relevant Authentication and Track &Trace projects, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.

Conclusion: A basic co-operation with affected industries allows government agencies, when implementing the TPD, to benefit from industry's systems, expertise and budgets.

4. **Preventive/ predictive systems** Combining repressive measures and preventive measures is highly effective. Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective. Preventive/predictive systems can be a key tool for different agencies involved in fighting back against illicit trade.
   Important structured data sources are:
   - Digital Track & Trace systems from product suppliers and/or governments: If such systems apply digital coding on the products on the level of the SSU (smallest sellable unit), they can gain a deep insight in the movements of legal and illegal goods in a country.
   - Consumers: Today's smartphone and App technology allow citizens to check the authenticity of a product they are about to purchase. Involving citizens will multiply the amount of data that can be fed into analytical systems.

   Technological conditions for such citizen involvement: digital coding of products on pack level, and the use open standards (Atos supports the use of GS-1 standards)

   Conclusion: the use of preventive/predictive analytical IT systems is highly effective to fight illicit trade, and should be stimulated.

EC Consultation – Atos written statements

Atos SE (Societas Europaea) is a leader in digital services with 2014 pro forma annual revenue of circa € 11 billion and 93,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. A trusted partner for governmental institutions in many European countries, Atos provide services in areas such as e-tax filing, defence/ intelligence/ security systems, electronic truck tolling, as well as intelligent electronic regulatory reporting systems.

Atos has set up a Global Centre of Competence Serialization that supports the local application of IT systems to effectively fight illicit trade. Through the Centre we have successfully implemented effective, IT based Product Authentication and Track & Trace solutions across several industries, from pharmaceutical to tobacco and luxury goods.

B.1.5.

Option 1: Option 1 provides several advantages compared to the other options. It is based on an outlined cooperation between the authorities and the private sector. Compared to the other options it allows for capturing industry key learnings and leveraging the existing methods and installed systems. The option is based on reusing the existing systems currently used by the industry. This increases feasibility and cost efficiency for all stakeholders. It also reduces system implementation lead time.
We see two key benefits of an outlined cooperation with the tobacco industry:

- Many different companies already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats.

That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.
The Atos Competence Centre was involved in relevant Authentication and Track & Trace projects in different industries, including tobacco, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.
It is imperative Option 1 is implemented and operated under stringent control and audit rules as defined and endorsed by the Authorities.

Option 2: While Option 2 could leverage the advantages related to an EU wide approach (i.e. leading to one harmonized system), we foresee serious issues with the technical and organizational feasibility of this scenario.
Given the EU market size of tobacco products and the related amount of events to be captured, the size and manageability of one EU data repository would be very challenging. Also the alignment of the member states is a complicating factor. We fear this will result in delays in implementation time and will

not lead to a user friendly system, with compromises on usability (ex. system response time) and functionality.
The suggestion in Section 8.3.1 'Key principles' to replicate data to the Member States will increase overall level of efforts, both for the involved Solution Providers and the Member States, and lead to a higher overall cost.
Section 8.3.1'Key principles' also states that the solution may be operated by one (or more) solution provider(s) implementing a community wide traceability system. It is likely this would in fact create a kind of monopoly position for this solution provider. The European and National authorities would become dependent on one single solution provider. This can have negative impact on the cost efficiency and will limit the dynamics of future innovation.
Option 2 therefor does not seem to be a very realistic scenario, as the alignment of all Member States and stakeholders will be challenging due to mentioned technical, economical, but also organizational inconveniences.

Option 3: This option would increase costs unnecessarily (cost of dbase replication), prevent economies of scale and is not a good basis for encouraging collaboration between Member States, which is a prime condition for effectively fighting illicit trade. Since the databases would be driven by the Member States, the exchange of information and view on the complete supply chain is becoming difficult. Moreover, it goes against the reality of illicit trade, which is for the largest part organized internationally, and is currently exploiting the inability of Member States to collaborate. It would also create substantial challenges for the manufacturers, who would need to abide several Member State defined solutions, with each solution potentially operated by a different solution provider. The chance is very likely that this Option will not achieve what it is supposed to be doing: reduce illicit trade.

Option 4:
In general terms we support the search for creating synergies by means of combining the traceability option with the security feature based upon integrating the Unique Identifier. A key condition to creating such a synergy is to opt for security features based on digital technologies.
Since all 4 suggested Options related to security features involve a paper based stamp in some format, this does not seem feasible: combining a 'digital' data carrier with a paper based security features will not lead to synergies. It will complicate matters, and create extra costs without providing value.
This Option demonstrates the main issue of how the study has been handled: It wrongly assumes that the only viable security features available today are 'traditional' technologies linked to paper stamps or banderoles. The study did not properly investigate the potential of digital alternatives. New technologies such as digital tax stamps or fingerprinting technology can provide a lot of advantages over paper based technologies.
Moreover, there is a lot of focus on the security features itself and less on the practicality of the proposed paper based security systems, which is a missed opportunity. Digital alternatives will support the activities from the stakeholders* fighting illicit trade a lot better, and will allow for better integration with T&T systems (*Customs, Tax Authorities, Border police, Criminal Police,…).
If not reevaluated, it will cause the current Option 4 to fail its purpose and not lead to the economies as described in Section 8.5 of the feasibility study.

B.2.5.

As a general comment we disagree with the report and analysis, which only focuses on traditional solutions, while not exploring innovative and new solutions. The potential benefits of technologies such

as digital stamps, fingerprint of the products pack or fingerprint of the authorized printers should have been analyzed in the report.
Instead, the report only focused on exploring security features based on paper-based stamps or labels, and suggesting in all 4 options that paper stamps are needed. These are often counterfeited and create a false sense of security, as it may only provide information about the label itself, not the product. The ambition of TPD, and what it is trying to achieve, requires the use of advanced technologies which enable the authentication of products based on the individual physical properties of the product. A key success factor will be the ability to provide authentication of the pack, not a stamp or a label. It is therefore important that the Commission orients itself to embracing and promoting new technologies.

C.1.1.

The feasibility study has only focused on assessing traditional 'paper based' security feature technologies. As referred to in Section 8.5.1 'Key Principles' of Tobacco Traceability Option 4, this is the key building block you could integrate with the 'digital' traceability solution to explore synergies. We refer to our relevant remarks under Section 4 in B.1.5 of this document, in which we state that the combination of a 'digital' data carrier with a paper based security features will not lead to synergies. We therefor suggest that 'digital' alternatives are properly evaluated in a follow up study.
The study fails to reflect on the practicality of the different Options, and how some of the key stakeholders* would benefit from the systems, or not (*Customs, Tax Authorities, Border police, Criminal Police who focus on fighting illicit trade). We are convinced that in case new technologies would have been considered, the benefit analysis would be substantially better. The current benefit analysis as described in Section 11.3 is simply generic and fails to provide tangible value to the Commission and the EU MS.
We agree with the finding of the report under Section 11.3.1 'Benefit Analysis' that it is likely that any combination of the 4 solution options will provide 'similar' results. We think however this result will be mediocre to poor in case new technologies are not adequately considered. We think this would be a missed opportunity. For example: the described 'traditional' tax stamps and overt security features have been around for many years but have not proved very successful for goods identification and fighting illicit trade. They are found to be copied easily, or removed from a legal pack to be used on smuggled products or counterfeited. The ambition of this feasibility study could have been to look for systems which could really make a difference, by using new technologies which are often already in use by different industries.
Furthermore the analysis misses out on assessing the potential impact of enhancing public awareness and actively engaging EU citizens, better field inspection methodologies and control, and the impact of strengthened law enforcement. How will the described Options either help or not in these areas?
Modern technology solutions could help combat counterfeiting and illicit trade. It requires the EU to go beyond what most Member States have been doing until now, and suggest the way forward is to evaluate the available new technologies. We therefore believe this study is a missed opportunity.
For example, taggant technology systems have a low implementation cost since it is integrated into the pack, while it reduces the risk for counterfeiting and fraud. Certain manufacturers and distributors have already installed this technology and are using it, providing potential economies of reusing this existing system. This has unfortunately not been considered in the analysis.

The costs related to Option 4 under 11.2.3 seem underestimated: based on the relevant experience of Atos syncing 2 separate solutions (one for printing and one for verifying) will lead to substantially higher implementing and operating costs.
Based on conversations with different Member States, we see as well that the Total Cost Of Ownership (TCO) linked to the use of tax stamps is generally underestimated (cost of transportation and storage, risk management of counterfeit,…)
Given the missed opportunity for studying the above described benefits, the costs and calculations as presented in 11.3.2 may be academic but bear limited value. We do not have insight on the modeling techniques and assumptions which have been mentioned under Section 11. Without this info it is not possible to provide further comments on Section 11.3.2.

D.2.

We recommend the use of GTIN and serial number as the unique code for the individual product/SKU level, and SGTIN for other packaging levels. For generation of a serialized Unique Identifier, we recommend a highly secure algorithm which takes into consideration the manufacturer, the individual product (SKU), based on a high level of randomization.

D.5.

We believe both machine and human readable codes are required:
A human readable code allows for every consumer to be involved in the process of verifying the authenticity of the product. It can also serve as a backup solution in case the machine readable code can't be read.
A machine readable code will help authorities to efficiently perform verifications. A machine readable code is essential during the manufacturing process, as a human readable code would not be able to support the printing at production speeds. A machine readable code is equally suited to support the aggregation process, which is at the heart of any effective track and trace offering. Machine readable codes could also be used by consumers with a smartphone, eliminating the risk of misreading the human readable code. A Covert Machine readable code also allows to include more information in the coding.

D.11.

We refer to our earlier remark that the feasibility study is only focused on assessing traditional 'paper based' security feature technologies. The report fails to assess alternative methods such as tear tape embedded with security features (which is used in many countries to carry covert, overt and forensic authentication technologies). Main advantage of this type of security feature is that it becomes an integral part of the existing packaging specification. This would reduce the impact and costs in terms of additional infrastructure requirements, and would be an alternative to the costly paper tax stamps, which are known to be easily copied or stolen.

D.13.

Based on the experience and expertise from Atos in the domain of Data management and storage, and reflecting on the requirements as described in Article 15 (8) of TPD, we point out the following important pillars related to Integration services & IT Security:

Integration services

To ensure an easy integration with the external world, the usage of proven market standards is for the envisaged system is important:

- Products are identified by an electronic Product Code (EPC)
- the specification EPCIS (Electronic Product Code Services Information Services) aiming to enable disparate applications to leverage Electronic Product Code (EPC) data via EPC-related data sharing, both within and across (enterprise and government) systems
- pack related information is stored in a machine readable code

From a technological point of view, the solution should be based on Service-Oriented Architecture concepts and provide external interfaces using well-accepted standards (Web Services, WSDL, SOAP) and wide-spread protocols (FTP, HTTP, HTTPS).

IT security : Measures to protect the system and its connections against threats from outside

Due to the amount and sensitivity of the manufacturing data, the system will have a special need for data protection and protection of the system itself, requiring the Data Management Provider to have an ample expertise in planning, implementing and operating security-critical systems.

In order to design an optimized protection the following activities typically need to be performed:

1. Analysis of protection requirement* with regard to the targets of confidentiality, integrity and availability
2. Implementation of an ISMS (Information Security Management System)
3. Implementation of the actual security systems (see listings below)

Step 1 will ensure that we plan for the necessary protection levels and do not overprotect certain areas while neglecting others. Results from the analysis will determine the implementation steps 2 and 3.

Step 2: The Information Security Management System (ISMS) describes all procedures and rules to control, maintain and improve IT-Security. It is absolutely crucial to maintain a consistent protection against the different types of threats. A proven and audited standard ISMS is vital, based upon which extensions and changes to this Standard would have to be implemented.

Step 3: The Technical Security Systems will enforce security rules and enable the automated detection of deviations. For the envisaged system in scope we consider the following security systems to be indispensable:

- Firewall/Proxy Services
- IAM – Identity and Access Management
- IDS/IPS – Intrusion Detection/Prevention System
- Full and strong Data Encryption for all data in transfer outside the datacenter
- Vulnerability Management Services
- Physical high security measures (Atos datacenter standard)

Additional technical systems/measures will be considered depending on the outcome of the protection requirements*:

- Web Application Firewall
- Data Encryption for data in storage, e.g. in the database
- Full and strong Data Encryption for data in transfer inside the datacenter
- DLP – Data Loss Prevention
- SIEM - Security Information and Event Management

- Security Operations Center to handle events from DLP and SIEM
- Strong Authentication by hardware-based digital certificates

In the design and the implementation of such Security Systems, we recommend to follow the relevant standards and all legal regulations (e.g. ISO 2700x). Moreover it is self-evident that in the course of the operations the security system will be audited internally and externally.

IT security : Measures to achieve a strict separation of access to the data of different stakeholders

The ISMS and its technical measures also ensure the high protection levels within the system. Requirements for a strict separation of access to data from the manufacturers will be ensured by employing the following measures:

- Design Measures (the design of the system will enforce that accidental or intentional access violations either from stakeholders or privileged users cannot take place)
    1. Incorporating a robust cloud security assessment service into the analysis of the protection requirements
    2. Designing and implementing an Identity and Access Management
    3. Application architecture supporting multi-tenancy
    4. The business logic has to be built to support multi-tenancy
    5. Physical separation of the databases
    6. Data encryption services inside the data center
- Operations Measures (detecting deviations during operations)
    1. DLP -Data Loss Prevention
    2. SIEM -Security Information and Event Management
    3. SOC - Security Operations Center

D.15.

Both a) and b) could provide reporting and query tools. The provider of data storage services could perform the role of certified interface to the Member States authorities and serve as trusted entity, independent from the manufacturers.

We consider the development of reporting and query tools to be a key consideration for making the TPD a success. It is important to develop and provide to the relevant authorities and stakeholders a highly secured Analysis platform, delivering Preventive IT Systems. This platform would provide advanced analytical capabilities, like anomaly detection, predictive analytics and advanced pattern recognition and would be supported by experts with in-depth vertical domain know-how, paired with advanced analytics skills.

Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective.
This platform would be based on handling different types of information flows consisting of structured and unstructured data, which will, by means of data mining and analytics, lead to useful information.
The main benefits and outcome would be useful information to be used by the relevant authorities for

- ► Spotting and predicting illicit trade patterns
- ► Focusing on critical cases and “big fishes”
- ► Improving efficiency and effectiveness for Law Enforcement

► Improving collaboration with other entities

D.17.

Any proposed tracking and tracing solution for the TPD must have at its heart the ability to uniquely identify products. Unique identification is not only important for the product authentication purposes, but should also support an aggregation process, and build a relationship between different levels of packaging, which is already part of the traditional manufacturing practice.
Interoperability is another key feature. There is a wide choice of existing coding systems suppliers which are supporting manufacturers across the EU and globally, allowing for reuse of the equipment at line level and systems as a whole at governmental or factory level. It is therefore recommended that any adopted tracking and tracing solution for use with the TPD would facilitate the reuse, if compliant with Open Standards.
Allowing as many suppliers as possible to support manufacturers and governments is the only practical approach to gain a successful outcome.
The main items to effectively fight illicit trade: Collaboration between industries and organizations, sharing knowledge and leveraging best practices, promoting open standards and technical development, and leverage the use of new technologies.

The key considerations regarding the implementation of the Tobacco Products Directive from Atos are:

1. **Technology should be part of a broader strategy.** Track &Trace systems can assist authorities to fight the growing issue of illicit tobacco trade. Today's technologies provide substantial improvement opportunities, but should be part of a broader strategy that also includes other measures: effective cross-border data exchange, interactive inspections, intelligent analysis tools, and enforcement in the field.
   Conclusion: technology should be embedded in a broader strategy

2. **International co-operation and information exchange.** Illicit trade is a cross-border phenomenon. The TPD can only be effectively implemented if member states and their enforcement agencies can co-operate and exchange information. The technological consequence of the need for co-operation and exchange is the choice for open standards-based systems. Atos supports the use of GS1 standards to identify products, capture the information at key points in the supply chain and then share the information seamlessly among stakeholders. This approach will ensure:
   - Easy integration with and interoperability between existing governmental systems, enforcement agencies and even industry
   - The ability to work cross border and effectively fight illicit trade
   - Ability of governments to use standard smart-phones and scanning devices for in-field inspections. This reduces cost and complexity, and ensures easy system maintenance.
   - Dependence on one specific supplier or use of proprietary systems will not lead to cost and system efficiency, and will limit future innovation
   - Avoid a European patchwork of standards that will raise the cost and complexity and making an effective tobacco control impossible

   Conclusion: open standards-based systems allow international co-operation and information exchange.

3. **Co-operation with private sector.** We see two benefits of a basic co-operation between the authorities and the private sector, in relation to the implementation of the TPD.

- Many major tobacco suppliers already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats. That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.

The Atos Competence Centre was involved in relevant Authentication and Track &Trace projects, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.

Conclusion: A basic co-operation with affected industries allows government agencies, when implementing the TPD, to benefit from industry's systems, expertise and budgets.

4. **Preventive/ predictive systems** Combining repressive measures and preventive measures is highly effective. Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective. Preventive/predictive systems can be a key tool for different agencies involved in fighting back against illicit trade.
   Important structured data sources are:
   - Digital Track & Trace systems from product suppliers and/or governments: If such systems apply digital coding on the products on the level of the SSU (smallest sellable unit), they can gain a deep insight in the movements of legal and illegal goods in a country.
   - Consumers: Today's smartphone and App technology allow citizens to check the authenticity of a product they are about to purchase. Involving citizens will multiply the amount of data that can be fed into analytical systems.

   Technological conditions for such citizen involvement: digital coding of products on pack level, and the use open standards (Atos supports the use of GS-1 standards)

   Conclusion: the use of preventive/predictive analytical IT systems is highly effective to fight illicit trade, and should be stimulated.

Attachment D.11

EC Consultation – Atos written statements

Atos SE (Societas Europaea) is a leader in digital services with 2014 pro forma annual revenue of circa € 11 billion and 93,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. A trusted partner for governmental institutions in many European countries, Atos provide services in areas such as e-tax filing, defence/ intelligence/ security systems, electronic truck tolling, as well as intelligent electronic regulatory reporting systems.

Atos has set up a Global Centre of Competence Serialization that supports the local application of IT systems to effectively fight illicit trade. Through the Centre we have successfully implemented effective, IT based Product Authentication and Track & Trace solutions across several industries, from pharmaceutical to tobacco and luxury goods.

B.1.5.

Option 1: Option 1 provides several advantages compared to the other options. It is based on an outlined cooperation between the authorities and the private sector. Compared to the other options it allows for capturing industry key learnings and leveraging the existing methods and installed systems. The option is based on reusing the existing systems currently used by the industry. This increases feasibility and cost efficiency for all stakeholders. It also reduces system implementation lead time.
We see two key benefits of an outlined cooperation with the tobacco industry:

- Many different companies already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats.

That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.
The Atos Competence Centre was involved in relevant Authentication and Track & Trace projects in different industries, including tobacco, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.
It is imperative Option 1 is implemented and operated under stringent control and audit rules as defined and endorsed by the Authorities.

Option 2: While Option 2 could leverage the advantages related to an EU wide approach (i.e. leading to one harmonized system), we foresee serious issues with the technical and organizational feasibility of this scenario.
Given the EU market size of tobacco products and the related amount of events to be captured, the size and manageability of one EU data repository would be very challenging. Also the alignment of the member states is a complicating factor. We fear this will result in delays in implementation time and will

not lead to a user friendly system, with compromises on usability (ex. system response time) and functionality.
The suggestion in Section 8.3.1 'Key principles' to replicate data to the Member States will increase overall level of efforts, both for the involved Solution Providers and the Member States, and lead to a higher overall cost.
Section 8.3.1'Key principles' also states that the solution may be operated by one (or more) solution provider(s) implementing a community wide traceability system. It is likely this would in fact create a kind of monopoly position for this solution provider. The European and National authorities would become dependent on one single solution provider. This can have negative impact on the cost efficiency and will limit the dynamics of future innovation.
Option 2 therefor does not seem to be a very realistic scenario, as the alignment of all Member States and stakeholders will be challenging due to mentioned technical, economical, but also organizational inconveniences.

Option 3: This option would increase costs unnecessarily (cost of dbase replication), prevent economies of scale and is not a good basis for encouraging collaboration between Member States, which is a prime condition for effectively fighting illicit trade. Since the databases would be driven by the Member States, the exchange of information and view on the complete supply chain is becoming difficult. Moreover, it goes against the reality of illicit trade, which is for the largest part organized internationally, and is currently exploiting the inability of Member States to collaborate. It would also create substantial challenges for the manufacturers, who would need to abide several Member State defined solutions, with each solution potentially operated by a different solution provider. The chance is very likely that this Option will not achieve what it is supposed to be doing: reduce illicit trade.

Option 4:
In general terms we support the search for creating synergies by means of combining the traceability option with the security feature based upon integrating the Unique Identifier. A key condition to creating such a synergy is to opt for security features based on digital technologies.
Since all 4 suggested Options related to security features involve a paper based stamp in some format, this does not seem feasible: combining a 'digital' data carrier with a paper based security features will not lead to synergies. It will complicate matters, and create extra costs without providing value.
This Option demonstrates the main issue of how the study has been handled: It wrongly assumes that the only viable security features available today are 'traditional' technologies linked to paper stamps or banderoles. The study did not properly investigate the potential of digital alternatives. New technologies such as digital tax stamps or fingerprinting technology can provide a lot of advantages over paper based technologies.
Moreover, there is a lot of focus on the security features itself and less on the practicality of the proposed paper based security systems, which is a missed opportunity. Digital alternatives will support the activities from the stakeholders* fighting illicit trade a lot better, and will allow for better integration with T&T systems (*Customs, Tax Authorities, Border police, Criminal Police,…).
If not reevaluated, it will cause the current Option 4 to fail its purpose and not lead to the economies as described in Section 8.5 of the feasibility study.

B.2.5.

As a general comment we disagree with the report and analysis, which only focuses on traditional solutions, while not exploring innovative and new solutions. The potential benefits of technologies such

as digital stamps, fingerprint of the products pack or fingerprint of the authorized printers should have been analyzed in the report.
Instead, the report only focused on exploring security features based on paper-based stamps or labels, and suggesting in all 4 options that paper stamps are needed. These are often counterfeited and create a false sense of security, as it may only provide information about the label itself, not the product. The ambition of TPD, and what it is trying to achieve, requires the use of advanced technologies which enable the authentication of products based on the individual physical properties of the product. A key success factor will be the ability to provide authentication of the pack, not a stamp or a label. It is therefore important that the Commission orients itself to embracing and promoting new technologies.

C.1.1.

The feasibility study has only focused on assessing traditional 'paper based' security feature technologies. As referred to in Section 8.5.1 'Key Principles' of Tobacco Traceability Option 4, this is the key building block you could integrate with the 'digital' traceability solution to explore synergies. We refer to our relevant remarks under Section 4 in B.1.5 of this document, in which we state that the combination of a 'digital' data carrier with a paper based security features will not lead to synergies. We therefor suggest that 'digital' alternatives are properly evaluated in a follow up study.
The study fails to reflect on the practicality of the different Options, and how some of the key stakeholders* would benefit from the systems, or not (*Customs, Tax Authorities, Border police, Criminal Police who focus on fighting illicit trade). We are convinced that in case new technologies would have been considered, the benefit analysis would be substantially better. The current benefit analysis as described in Section 11.3 is simply generic and fails to provide tangible value to the Commission and the EU MS.
We agree with the finding of the report under Section 11.3.1 'Benefit Analysis' that it is likely that any combination of the 4 solution options will provide 'similar' results. We think however this result will be mediocre to poor in case new technologies are not adequately considered. We think this would be a missed opportunity. For example: the described 'traditional' tax stamps and overt security features have been around for many years but have not proved very successful for goods identification and fighting illicit trade. They are found to be copied easily, or removed from a legal pack to be used on smuggled products or counterfeited. The ambition of this feasibility study could have been to look for systems which could really make a difference, by using new technologies which are often already in use by different industries.
Furthermore the analysis misses out on assessing the potential impact of enhancing public awareness and actively engaging EU citizens, better field inspection methodologies and control, and the impact of strengthened law enforcement. How will the described Options either help or not in these areas?
Modern technology solutions could help combat counterfeiting and illicit trade. It requires the EU to go beyond what most Member States have been doing until now, and suggest the way forward is to evaluate the available new technologies. We therefore believe this study is a missed opportunity.
For example, taggant technology systems have a low implementation cost since it is integrated into the pack, while it reduces the risk for counterfeiting and fraud. Certain manufacturers and distributors have already installed this technology and are using it, providing potential economies of reusing this existing system. This has unfortunately not been considered in the analysis.

The costs related to Option 4 under 11.2.3 seem underestimated: based on the relevant experience of Atos syncing 2 separate solutions (one for printing and one for verifying) will lead to substantially higher implementing and operating costs.
Based on conversations with different Member States, we see as well that the Total Cost Of Ownership (TCO) linked to the use of tax stamps is generally underestimated (cost of transportation and storage, risk management of counterfeit,…)
Given the missed opportunity for studying the above described benefits, the costs and calculations as presented in 11.3.2 may be academic but bear limited value. We do not have insight on the modeling techniques and assumptions which have been mentioned under Section 11. Without this info it is not possible to provide further comments on Section 11.3.2.

D.2.

We recommend the use of GTIN and serial number as the unique code for the individual product/SKU level, and SGTIN for other packaging levels. For generation of a serialized Unique Identifier, we recommend a highly secure algorithm which takes into consideration the manufacturer, the individual product (SKU), based on a high level of randomization.

D.5.

We believe both machine and human readable codes are required:
A human readable code allows for every consumer to be involved in the process of verifying the authenticity of the product. It can also serve as a backup solution in case the machine readable code can't be read.
A machine readable code will help authorities to efficiently perform verifications. A machine readable code is essential during the manufacturing process, as a human readable code would not be able to support the printing at production speeds. A machine readable code is equally suited to support the aggregation process, which is at the heart of any effective track and trace offering. Machine readable codes could also be used by consumers with a smartphone, eliminating the risk of misreading the human readable code. A Covert Machine readable code also allows to include more information in the coding.

D.11.

We refer to our earlier remark that the feasibility study is only focused on assessing traditional 'paper based' security feature technologies. The report fails to assess alternative methods such as tear tape embedded with security features (which is used in many countries to carry covert, overt and forensic authentication technologies). Main advantage of this type of security feature is that it becomes an integral part of the existing packaging specification. This would reduce the impact and costs in terms of additional infrastructure requirements, and would be an alternative to the costly paper tax stamps, which are known to be easily copied or stolen.

D.13.

Based on the experience and expertise from Atos in the domain of Data management and storage, and reflecting on the requirements as described in Article 15 (8) of TPD, we point out the following important pillars related to Integration services & IT Security:

Integration services

To ensure an easy integration with the external world, the usage of proven market standards is for the envisaged system is important:

- Products are identified by an electronic Product Code (EPC)
- the specification EPCIS (Electronic Product Code Services Information Services) aiming to enable disparate applications to leverage Electronic Product Code (EPC) data via EPC-related data sharing, both within and across (enterprise and government) systems
- pack related information is stored in a machine readable code

From a technological point of view, the solution should be based on Service-Oriented Architecture concepts and provide external interfaces using well-accepted standards (Web Services, WSDL, SOAP) and wide-spread protocols (FTP, HTTP, HTTPS).

IT security : Measures to protect the system and its connections against threats from outside

Due to the amount and sensitivity of the manufacturing data, the system will have a special need for data protection and protection of the system itself, requiring the Data Management Provider to have an ample expertise in planning, implementing and operating security-critical systems.

In order to design an optimized protection the following activities typically need to be performed:

1. Analysis of protection requirement* with regard to the targets of confidentiality, integrity and availability
2. Implementation of an ISMS (Information Security Management System)
3. Implementation of the actual security systems (see listings below)

Step 1 will ensure that we plan for the necessary protection levels and do not overprotect certain areas while neglecting others. Results from the analysis will determine the implementation steps 2 and 3.

Step 2: The Information Security Management System (ISMS) describes all procedures and rules to control, maintain and improve IT-Security. It is absolutely crucial to maintain a consistent protection against the different types of threats. A proven and audited standard ISMS is vital, based upon which extensions and changes to this Standard would have to be implemented.

Step 3: The Technical Security Systems will enforce security rules and enable the automated detection of deviations. For the envisaged system in scope we consider the following security systems to be indispensable:

- Firewall/Proxy Services
- IAM – Identity and Access Management
- IDS/IPS – Intrusion Detection/Prevention System
- Full and strong Data Encryption for all data in transfer outside the datacenter
- Vulnerability Management Services
- Physical high security measures (Atos datacenter standard)

Additional technical systems/measures will be considered depending on the outcome of the protection requirements*:

- Web Application Firewall
- Data Encryption for data in storage, e.g. in the database
- Full and strong Data Encryption for data in transfer inside the datacenter
- DLP – Data Loss Prevention
- SIEM - Security Information and Event Management

- Security Operations Center to handle events from DLP and SIEM
- Strong Authentication by hardware-based digital certificates

In the design and the implementation of such Security Systems, we recommend to follow the relevant standards and all legal regulations (e.g. ISO 2700x). Moreover it is self-evident that in the course of the operations the security system will be audited internally and externally.

IT security : Measures to achieve a strict separation of access to the data of different stakeholders

The ISMS and its technical measures also ensure the high protection levels within the system. Requirements for a strict separation of access to data from the manufacturers will be ensured by employing the following measures:

- Design Measures (the design of the system will enforce that accidental or intentional access violations either from stakeholders or privileged users cannot take place)
    1. Incorporating a robust cloud security assessment service into the analysis of the protection requirements
    2. Designing and implementing an Identity and Access Management
    3. Application architecture supporting multi-tenancy
    4. The business logic has to be built to support multi-tenancy
    5. Physical separation of the databases
    6. Data encryption services inside the data center
- Operations Measures (detecting deviations during operations)
    1. DLP -Data Loss Prevention
    2. SIEM -Security Information and Event Management
    3. SOC - Security Operations Center

D.15.

Both a) and b) could provide reporting and query tools. The provider of data storage services could perform the role of certified interface to the Member States authorities and serve as trusted entity, independent from the manufacturers.

We consider the development of reporting and query tools to be a key consideration for making the TPD a success. It is important to develop and provide to the relevant authorities and stakeholders a highly secured Analysis platform, delivering Preventive IT Systems. This platform would provide advanced analytical capabilities, like anomaly detection, predictive analytics and advanced pattern recognition and would be supported by experts with in-depth vertical domain know-how, paired with advanced analytics skills.

Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective.
This platform would be based on handling different types of information flows consisting of structured and unstructured data, which will, by means of data mining and analytics, lead to useful information.
The main benefits and outcome would be useful information to be used by the relevant authorities for

- ► Spotting and predicting illicit trade patterns
- ► Focusing on critical cases and “big fishes”
- ► Improving efficiency and effectiveness for Law Enforcement

► Improving collaboration with other entities

D.17.

Any proposed tracking and tracing solution for the TPD must have at its heart the ability to uniquely identify products. Unique identification is not only important for the product authentication purposes, but should also support an aggregation process, and build a relationship between different levels of packaging, which is already part of the traditional manufacturing practice.
Interoperability is another key feature. There is a wide choice of existing coding systems suppliers which are supporting manufacturers across the EU and globally, allowing for reuse of the equipment at line level and systems as a whole at governmental or factory level. It is therefore recommended that any adopted tracking and tracing solution for use with the TPD would facilitate the reuse, if compliant with Open Standards.
Allowing as many suppliers as possible to support manufacturers and governments is the only practical approach to gain a successful outcome.
The main items to effectively fight illicit trade: Collaboration between industries and organizations, sharing knowledge and leveraging best practices, promoting open standards and technical development, and leverage the use of new technologies.

The key considerations regarding the implementation of the Tobacco Products Directive from Atos are:

1. **Technology should be part of a broader strategy.** Track &Trace systems can assist authorities to fight the growing issue of illicit tobacco trade. Today's technologies provide substantial improvement opportunities, but should be part of a broader strategy that also includes other measures: effective cross-border data exchange, interactive inspections, intelligent analysis tools, and enforcement in the field.
   Conclusion: technology should be embedded in a broader strategy

2. **International co-operation and information exchange.** Illicit trade is a cross-border phenomenon. The TPD can only be effectively implemented if member states and their enforcement agencies can co-operate and exchange information. The technological consequence of the need for co-operation and exchange is the choice for open standards-based systems. Atos supports the use of GS1 standards to identify products, capture the information at key points in the supply chain and then share the information seamlessly among stakeholders. This approach will ensure:
   - Easy integration with and interoperability between existing governmental systems, enforcement agencies and even industry
   - The ability to work cross border and effectively fight illicit trade
   - Ability of governments to use standard smart-phones and scanning devices for in-field inspections. This reduces cost and complexity, and ensures easy system maintenance.
   - Dependence on one specific supplier or use of proprietary systems will not lead to cost and system efficiency, and will limit future innovation
   - Avoid a European patchwork of standards that will raise the cost and complexity and making an effective tobacco control impossible

   Conclusion: open standards-based systems allow international co-operation and information exchange.

3. **Co-operation with private sector.** We see two benefits of a basic co-operation between the authorities and the private sector, in relation to the implementation of the TPD.

- Many major tobacco suppliers already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats. That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.

The Atos Competence Centre was involved in relevant Authentication and Track &Trace projects, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.

Conclusion: A basic co-operation with affected industries allows government agencies, when implementing the TPD, to benefit from industry's systems, expertise and budgets.

4. **Preventive/ predictive systems** Combining repressive measures and preventive measures is highly effective. Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective. Preventive/predictive systems can be a key tool for different agencies involved in fighting back against illicit trade.
   Important structured data sources are:
   - Digital Track & Trace systems from product suppliers and/or governments: If such systems apply digital coding on the products on the level of the SSU (smallest sellable unit), they can gain a deep insight in the movements of legal and illegal goods in a country.
   - Consumers: Today's smartphone and App technology allow citizens to check the authenticity of a product they are about to purchase. Involving citizens will multiply the amount of data that can be fed into analytical systems.

   Technological conditions for such citizen involvement: digital coding of products on pack level, and the use open standards (Atos supports the use of GS-1 standards)

   Conclusion: the use of preventive/predictive analytical IT systems is highly effective to fight illicit trade, and should be stimulated.

EC Consultation – Atos written statements

Atos SE (Societas Europaea) is a leader in digital services with 2014 pro forma annual revenue of circa € 11 billion and 93,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. A trusted partner for governmental institutions in many European countries, Atos provide services in areas such as e-tax filing, defence/ intelligence/ security systems, electronic truck tolling, as well as intelligent electronic regulatory reporting systems.

Atos has set up a Global Centre of Competence Serialization that supports the local application of IT systems to effectively fight illicit trade. Through the Centre we have successfully implemented effective, IT based Product Authentication and Track & Trace solutions across several industries, from pharmaceutical to tobacco and luxury goods.

B.1.5.

Option 1: Option 1 provides several advantages compared to the other options. It is based on an outlined cooperation between the authorities and the private sector. Compared to the other options it allows for capturing industry key learnings and leveraging the existing methods and installed systems. The option is based on reusing the existing systems currently used by the industry. This increases feasibility and cost efficiency for all stakeholders. It also reduces system implementation lead time.
We see two key benefits of an outlined cooperation with the tobacco industry:

- Many different companies already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats.

That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.
The Atos Competence Centre was involved in relevant Authentication and Track & Trace projects in different industries, including tobacco, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.
It is imperative Option 1 is implemented and operated under stringent control and audit rules as defined and endorsed by the Authorities.

Option 2: While Option 2 could leverage the advantages related to an EU wide approach (i.e. leading to one harmonized system), we foresee serious issues with the technical and organizational feasibility of this scenario.
Given the EU market size of tobacco products and the related amount of events to be captured, the size and manageability of one EU data repository would be very challenging. Also the alignment of the member states is a complicating factor. We fear this will result in delays in implementation time and will

not lead to a user friendly system, with compromises on usability (ex. system response time) and functionality.
The suggestion in Section 8.3.1 'Key principles' to replicate data to the Member States will increase overall level of efforts, both for the involved Solution Providers and the Member States, and lead to a higher overall cost.
Section 8.3.1'Key principles' also states that the solution may be operated by one (or more) solution provider(s) implementing a community wide traceability system. It is likely this would in fact create a kind of monopoly position for this solution provider. The European and National authorities would become dependent on one single solution provider. This can have negative impact on the cost efficiency and will limit the dynamics of future innovation.
Option 2 therefor does not seem to be a very realistic scenario, as the alignment of all Member States and stakeholders will be challenging due to mentioned technical, economical, but also organizational inconveniences.

Option 3: This option would increase costs unnecessarily (cost of dbase replication), prevent economies of scale and is not a good basis for encouraging collaboration between Member States, which is a prime condition for effectively fighting illicit trade. Since the databases would be driven by the Member States, the exchange of information and view on the complete supply chain is becoming difficult. Moreover, it goes against the reality of illicit trade, which is for the largest part organized internationally, and is currently exploiting the inability of Member States to collaborate. It would also create substantial challenges for the manufacturers, who would need to abide several Member State defined solutions, with each solution potentially operated by a different solution provider. The chance is very likely that this Option will not achieve what it is supposed to be doing: reduce illicit trade.

Option 4:
In general terms we support the search for creating synergies by means of combining the traceability option with the security feature based upon integrating the Unique Identifier. A key condition to creating such a synergy is to opt for security features based on digital technologies.
Since all 4 suggested Options related to security features involve a paper based stamp in some format, this does not seem feasible: combining a 'digital' data carrier with a paper based security features will not lead to synergies. It will complicate matters, and create extra costs without providing value.
This Option demonstrates the main issue of how the study has been handled: It wrongly assumes that the only viable security features available today are 'traditional' technologies linked to paper stamps or banderoles. The study did not properly investigate the potential of digital alternatives. New technologies such as digital tax stamps or fingerprinting technology can provide a lot of advantages over paper based technologies.
Moreover, there is a lot of focus on the security features itself and less on the practicality of the proposed paper based security systems, which is a missed opportunity. Digital alternatives will support the activities from the stakeholders* fighting illicit trade a lot better, and will allow for better integration with T&T systems (*Customs, Tax Authorities, Border police, Criminal Police,…).
If not reevaluated, it will cause the current Option 4 to fail its purpose and not lead to the economies as described in Section 8.5 of the feasibility study.

B.2.5.

As a general comment we disagree with the report and analysis, which only focuses on traditional solutions, while not exploring innovative and new solutions. The potential benefits of technologies such

as digital stamps, fingerprint of the products pack or fingerprint of the authorized printers should have been analyzed in the report.
Instead, the report only focused on exploring security features based on paper-based stamps or labels, and suggesting in all 4 options that paper stamps are needed. These are often counterfeited and create a false sense of security, as it may only provide information about the label itself, not the product. The ambition of TPD, and what it is trying to achieve, requires the use of advanced technologies which enable the authentication of products based on the individual physical properties of the product. A key success factor will be the ability to provide authentication of the pack, not a stamp or a label. It is therefore important that the Commission orients itself to embracing and promoting new technologies.

C.1.1.

The feasibility study has only focused on assessing traditional 'paper based' security feature technologies. As referred to in Section 8.5.1 'Key Principles' of Tobacco Traceability Option 4, this is the key building block you could integrate with the 'digital' traceability solution to explore synergies. We refer to our relevant remarks under Section 4 in B.1.5 of this document, in which we state that the combination of a 'digital' data carrier with a paper based security features will not lead to synergies. We therefor suggest that 'digital' alternatives are properly evaluated in a follow up study.
The study fails to reflect on the practicality of the different Options, and how some of the key stakeholders* would benefit from the systems, or not (*Customs, Tax Authorities, Border police, Criminal Police who focus on fighting illicit trade). We are convinced that in case new technologies would have been considered, the benefit analysis would be substantially better. The current benefit analysis as described in Section 11.3 is simply generic and fails to provide tangible value to the Commission and the EU MS.
We agree with the finding of the report under Section 11.3.1 'Benefit Analysis' that it is likely that any combination of the 4 solution options will provide 'similar' results. We think however this result will be mediocre to poor in case new technologies are not adequately considered. We think this would be a missed opportunity. For example: the described 'traditional' tax stamps and overt security features have been around for many years but have not proved very successful for goods identification and fighting illicit trade. They are found to be copied easily, or removed from a legal pack to be used on smuggled products or counterfeited. The ambition of this feasibility study could have been to look for systems which could really make a difference, by using new technologies which are often already in use by different industries.
Furthermore the analysis misses out on assessing the potential impact of enhancing public awareness and actively engaging EU citizens, better field inspection methodologies and control, and the impact of strengthened law enforcement. How will the described Options either help or not in these areas?
Modern technology solutions could help combat counterfeiting and illicit trade. It requires the EU to go beyond what most Member States have been doing until now, and suggest the way forward is to evaluate the available new technologies. We therefore believe this study is a missed opportunity.
For example, taggant technology systems have a low implementation cost since it is integrated into the pack, while it reduces the risk for counterfeiting and fraud. Certain manufacturers and distributors have already installed this technology and are using it, providing potential economies of reusing this existing system. This has unfortunately not been considered in the analysis.

The costs related to Option 4 under 11.2.3 seem underestimated: based on the relevant experience of Atos syncing 2 separate solutions (one for printing and one for verifying) will lead to substantially higher implementing and operating costs.
Based on conversations with different Member States, we see as well that the Total Cost Of Ownership (TCO) linked to the use of tax stamps is generally underestimated (cost of transportation and storage, risk management of counterfeit,…)
Given the missed opportunity for studying the above described benefits, the costs and calculations as presented in 11.3.2 may be academic but bear limited value. We do not have insight on the modeling techniques and assumptions which have been mentioned under Section 11. Without this info it is not possible to provide further comments on Section 11.3.2.

D.2.

We recommend the use of GTIN and serial number as the unique code for the individual product/SKU level, and SGTIN for other packaging levels. For generation of a serialized Unique Identifier, we recommend a highly secure algorithm which takes into consideration the manufacturer, the individual product (SKU), based on a high level of randomization.

D.5.

We believe both machine and human readable codes are required:
A human readable code allows for every consumer to be involved in the process of verifying the authenticity of the product. It can also serve as a backup solution in case the machine readable code can't be read.
A machine readable code will help authorities to efficiently perform verifications. A machine readable code is essential during the manufacturing process, as a human readable code would not be able to support the printing at production speeds. A machine readable code is equally suited to support the aggregation process, which is at the heart of any effective track and trace offering. Machine readable codes could also be used by consumers with a smartphone, eliminating the risk of misreading the human readable code. A Covert Machine readable code also allows to include more information in the coding.

D.11.

We refer to our earlier remark that the feasibility study is only focused on assessing traditional 'paper based' security feature technologies. The report fails to assess alternative methods such as tear tape embedded with security features (which is used in many countries to carry covert, overt and forensic authentication technologies). Main advantage of this type of security feature is that it becomes an integral part of the existing packaging specification. This would reduce the impact and costs in terms of additional infrastructure requirements, and would be an alternative to the costly paper tax stamps, which are known to be easily copied or stolen.

D.13.

Based on the experience and expertise from Atos in the domain of Data management and storage, and reflecting on the requirements as described in Article 15 (8) of TPD, we point out the following important pillars related to Integration services & IT Security:

Integration services

To ensure an easy integration with the external world, the usage of proven market standards is for the envisaged system is important:

- Products are identified by an electronic Product Code (EPC)
- the specification EPCIS (Electronic Product Code Services Information Services) aiming to enable disparate applications to leverage Electronic Product Code (EPC) data via EPC-related data sharing, both within and across (enterprise and government) systems
- pack related information is stored in a machine readable code

From a technological point of view, the solution should be based on Service-Oriented Architecture concepts and provide external interfaces using well-accepted standards (Web Services, WSDL, SOAP) and wide-spread protocols (FTP, HTTP, HTTPS).

IT security : Measures to protect the system and its connections against threats from outside

Due to the amount and sensitivity of the manufacturing data, the system will have a special need for data protection and protection of the system itself, requiring the Data Management Provider to have an ample expertise in planning, implementing and operating security-critical systems.

In order to design an optimized protection the following activities typically need to be performed:

1. Analysis of protection requirement* with regard to the targets of confidentiality, integrity and availability
2. Implementation of an ISMS (Information Security Management System)
3. Implementation of the actual security systems (see listings below)

Step 1 will ensure that we plan for the necessary protection levels and do not overprotect certain areas while neglecting others. Results from the analysis will determine the implementation steps 2 and 3.

Step 2: The Information Security Management System (ISMS) describes all procedures and rules to control, maintain and improve IT-Security. It is absolutely crucial to maintain a consistent protection against the different types of threats. A proven and audited standard ISMS is vital, based upon which extensions and changes to this Standard would have to be implemented.

Step 3: The Technical Security Systems will enforce security rules and enable the automated detection of deviations. For the envisaged system in scope we consider the following security systems to be indispensable:

- Firewall/Proxy Services
- IAM – Identity and Access Management
- IDS/IPS – Intrusion Detection/Prevention System
- Full and strong Data Encryption for all data in transfer outside the datacenter
- Vulnerability Management Services
- Physical high security measures (Atos datacenter standard)

Additional technical systems/measures will be considered depending on the outcome of the protection requirements*:

- Web Application Firewall
- Data Encryption for data in storage, e.g. in the database
- Full and strong Data Encryption for data in transfer inside the datacenter
- DLP – Data Loss Prevention
- SIEM - Security Information and Event Management

- Security Operations Center to handle events from DLP and SIEM
- Strong Authentication by hardware-based digital certificates

In the design and the implementation of such Security Systems, we recommend to follow the relevant standards and all legal regulations (e.g. ISO 2700x). Moreover it is self-evident that in the course of the operations the security system will be audited internally and externally.

IT security : Measures to achieve a strict separation of access to the data of different stakeholders

The ISMS and its technical measures also ensure the high protection levels within the system. Requirements for a strict separation of access to data from the manufacturers will be ensured by employing the following measures:

- Design Measures (the design of the system will enforce that accidental or intentional access violations either from stakeholders or privileged users cannot take place)
    1. Incorporating a robust cloud security assessment service into the analysis of the protection requirements
    2. Designing and implementing an Identity and Access Management
    3. Application architecture supporting multi-tenancy
    4. The business logic has to be built to support multi-tenancy
    5. Physical separation of the databases
    6. Data encryption services inside the data center
- Operations Measures (detecting deviations during operations)
    1. DLP -Data Loss Prevention
    2. SIEM -Security Information and Event Management
    3. SOC - Security Operations Center

D.15.

Both a) and b) could provide reporting and query tools. The provider of data storage services could perform the role of certified interface to the Member States authorities and serve as trusted entity, independent from the manufacturers.

We consider the development of reporting and query tools to be a key consideration for making the TPD a success. It is important to develop and provide to the relevant authorities and stakeholders a highly secured Analysis platform, delivering Preventive IT Systems. This platform would provide advanced analytical capabilities, like anomaly detection, predictive analytics and advanced pattern recognition and would be supported by experts with in-depth vertical domain know-how, paired with advanced analytics skills.

Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective.
This platform would be based on handling different types of information flows consisting of structured and unstructured data, which will, by means of data mining and analytics, lead to useful information.
The main benefits and outcome would be useful information to be used by the relevant authorities for

- ► Spotting and predicting illicit trade patterns
- ► Focusing on critical cases and “big fishes”
- ► Improving efficiency and effectiveness for Law Enforcement

► Improving collaboration with other entities

D.17.

Any proposed tracking and tracing solution for the TPD must have at its heart the ability to uniquely identify products. Unique identification is not only important for the product authentication purposes, but should also support an aggregation process, and build a relationship between different levels of packaging, which is already part of the traditional manufacturing practice.
Interoperability is another key feature. There is a wide choice of existing coding systems suppliers which are supporting manufacturers across the EU and globally, allowing for reuse of the equipment at line level and systems as a whole at governmental or factory level. It is therefore recommended that any adopted tracking and tracing solution for use with the TPD would facilitate the reuse, if compliant with Open Standards.
Allowing as many suppliers as possible to support manufacturers and governments is the only practical approach to gain a successful outcome.
The main items to effectively fight illicit trade: Collaboration between industries and organizations, sharing knowledge and leveraging best practices, promoting open standards and technical development, and leverage the use of new technologies.

The key considerations regarding the implementation of the Tobacco Products Directive from Atos are:

1. **Technology should be part of a broader strategy.** Track &Trace systems can assist authorities to fight the growing issue of illicit tobacco trade. Today's technologies provide substantial improvement opportunities, but should be part of a broader strategy that also includes other measures: effective cross-border data exchange, interactive inspections, intelligent analysis tools, and enforcement in the field.
   Conclusion: technology should be embedded in a broader strategy

2. **International co-operation and information exchange.** Illicit trade is a cross-border phenomenon. The TPD can only be effectively implemented if member states and their enforcement agencies can co-operate and exchange information. The technological consequence of the need for co-operation and exchange is the choice for open standards-based systems. Atos supports the use of GS1 standards to identify products, capture the information at key points in the supply chain and then share the information seamlessly among stakeholders. This approach will ensure:
   - Easy integration with and interoperability between existing governmental systems, enforcement agencies and even industry
   - The ability to work cross border and effectively fight illicit trade
   - Ability of governments to use standard smart-phones and scanning devices for in-field inspections. This reduces cost and complexity, and ensures easy system maintenance.
   - Dependence on one specific supplier or use of proprietary systems will not lead to cost and system efficiency, and will limit future innovation
   - Avoid a European patchwork of standards that will raise the cost and complexity and making an effective tobacco control impossible

   Conclusion: open standards-based systems allow international co-operation and information exchange.

3. **Co-operation with private sector.** We see two benefits of a basic co-operation between the authorities and the private sector, in relation to the implementation of the TPD.

- Many major tobacco suppliers already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats. That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.

The Atos Competence Centre was involved in relevant Authentication and Track &Trace projects, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.

Conclusion: A basic co-operation with affected industries allows government agencies, when implementing the TPD, to benefit from industry's systems, expertise and budgets.

4. **Preventive/ predictive systems** Combining repressive measures and preventive measures is highly effective. Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective. Preventive/predictive systems can be a key tool for different agencies involved in fighting back against illicit trade.
   Important structured data sources are:
   - Digital Track & Trace systems from product suppliers and/or governments: If such systems apply digital coding on the products on the level of the SSU (smallest sellable unit), they can gain a deep insight in the movements of legal and illegal goods in a country.
   - Consumers: Today's smartphone and App technology allow citizens to check the authenticity of a product they are about to purchase. Involving citizens will multiply the amount of data that can be fed into analytical systems.

   Technological conditions for such citizen involvement: digital coding of products on pack level, and the use open standards (Atos supports the use of GS-1 standards)

   Conclusion: the use of preventive/predictive analytical IT systems is highly effective to fight illicit trade, and should be stimulated.

Attachment D.15

EC Consultation – Atos written statements

Atos SE (Societas Europaea) is a leader in digital services with 2014 pro forma annual revenue of circa € 11 billion and 93,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. A trusted partner for governmental institutions in many European countries, Atos provide services in areas such as e-tax filing, defence/ intelligence/ security systems, electronic truck tolling, as well as intelligent electronic regulatory reporting systems.

Atos has set up a Global Centre of Competence Serialization that supports the local application of IT systems to effectively fight illicit trade. Through the Centre we have successfully implemented effective, IT based Product Authentication and Track & Trace solutions across several industries, from pharmaceutical to tobacco and luxury goods.

B.1.5.

Option 1: Option 1 provides several advantages compared to the other options. It is based on an outlined cooperation between the authorities and the private sector. Compared to the other options it allows for capturing industry key learnings and leveraging the existing methods and installed systems. The option is based on reusing the existing systems currently used by the industry. This increases feasibility and cost efficiency for all stakeholders. It also reduces system implementation lead time.
We see two key benefits of an outlined cooperation with the tobacco industry:

- Many different companies already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats.

That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.
The Atos Competence Centre was involved in relevant Authentication and Track & Trace projects in different industries, including tobacco, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.
It is imperative Option 1 is implemented and operated under stringent control and audit rules as defined and endorsed by the Authorities.

Option 2: While Option 2 could leverage the advantages related to an EU wide approach (i.e. leading to one harmonized system), we foresee serious issues with the technical and organizational feasibility of this scenario.
Given the EU market size of tobacco products and the related amount of events to be captured, the size and manageability of one EU data repository would be very challenging. Also the alignment of the member states is a complicating factor. We fear this will result in delays in implementation time and will

not lead to a user friendly system, with compromises on usability (ex. system response time) and functionality.
The suggestion in Section 8.3.1 'Key principles' to replicate data to the Member States will increase overall level of efforts, both for the involved Solution Providers and the Member States, and lead to a higher overall cost.
Section 8.3.1'Key principles' also states that the solution may be operated by one (or more) solution provider(s) implementing a community wide traceability system. It is likely this would in fact create a kind of monopoly position for this solution provider. The European and National authorities would become dependent on one single solution provider. This can have negative impact on the cost efficiency and will limit the dynamics of future innovation.
Option 2 therefor does not seem to be a very realistic scenario, as the alignment of all Member States and stakeholders will be challenging due to mentioned technical, economical, but also organizational inconveniences.

Option 3: This option would increase costs unnecessarily (cost of dbase replication), prevent economies of scale and is not a good basis for encouraging collaboration between Member States, which is a prime condition for effectively fighting illicit trade. Since the databases would be driven by the Member States, the exchange of information and view on the complete supply chain is becoming difficult. Moreover, it goes against the reality of illicit trade, which is for the largest part organized internationally, and is currently exploiting the inability of Member States to collaborate. It would also create substantial challenges for the manufacturers, who would need to abide several Member State defined solutions, with each solution potentially operated by a different solution provider. The chance is very likely that this Option will not achieve what it is supposed to be doing: reduce illicit trade.

Option 4:
In general terms we support the search for creating synergies by means of combining the traceability option with the security feature based upon integrating the Unique Identifier. A key condition to creating such a synergy is to opt for security features based on digital technologies.
Since all 4 suggested Options related to security features involve a paper based stamp in some format, this does not seem feasible: combining a 'digital' data carrier with a paper based security features will not lead to synergies. It will complicate matters, and create extra costs without providing value.
This Option demonstrates the main issue of how the study has been handled: It wrongly assumes that the only viable security features available today are 'traditional' technologies linked to paper stamps or banderoles. The study did not properly investigate the potential of digital alternatives. New technologies such as digital tax stamps or fingerprinting technology can provide a lot of advantages over paper based technologies.
Moreover, there is a lot of focus on the security features itself and less on the practicality of the proposed paper based security systems, which is a missed opportunity. Digital alternatives will support the activities from the stakeholders* fighting illicit trade a lot better, and will allow for better integration with T&T systems (*Customs, Tax Authorities, Border police, Criminal Police,…).
If not reevaluated, it will cause the current Option 4 to fail its purpose and not lead to the economies as described in Section 8.5 of the feasibility study.

B.2.5.

As a general comment we disagree with the report and analysis, which only focuses on traditional solutions, while not exploring innovative and new solutions. The potential benefits of technologies such

as digital stamps, fingerprint of the products pack or fingerprint of the authorized printers should have been analyzed in the report.
Instead, the report only focused on exploring security features based on paper-based stamps or labels, and suggesting in all 4 options that paper stamps are needed. These are often counterfeited and create a false sense of security, as it may only provide information about the label itself, not the product. The ambition of TPD, and what it is trying to achieve, requires the use of advanced technologies which enable the authentication of products based on the individual physical properties of the product. A key success factor will be the ability to provide authentication of the pack, not a stamp or a label. It is therefore important that the Commission orients itself to embracing and promoting new technologies.

C.1.1.

The feasibility study has only focused on assessing traditional 'paper based' security feature technologies. As referred to in Section 8.5.1 'Key Principles' of Tobacco Traceability Option 4, this is the key building block you could integrate with the 'digital' traceability solution to explore synergies. We refer to our relevant remarks under Section 4 in B.1.5 of this document, in which we state that the combination of a 'digital' data carrier with a paper based security features will not lead to synergies. We therefor suggest that 'digital' alternatives are properly evaluated in a follow up study.
The study fails to reflect on the practicality of the different Options, and how some of the key stakeholders* would benefit from the systems, or not (*Customs, Tax Authorities, Border police, Criminal Police who focus on fighting illicit trade). We are convinced that in case new technologies would have been considered, the benefit analysis would be substantially better. The current benefit analysis as described in Section 11.3 is simply generic and fails to provide tangible value to the Commission and the EU MS.
We agree with the finding of the report under Section 11.3.1 'Benefit Analysis' that it is likely that any combination of the 4 solution options will provide 'similar' results. We think however this result will be mediocre to poor in case new technologies are not adequately considered. We think this would be a missed opportunity. For example: the described 'traditional' tax stamps and overt security features have been around for many years but have not proved very successful for goods identification and fighting illicit trade. They are found to be copied easily, or removed from a legal pack to be used on smuggled products or counterfeited. The ambition of this feasibility study could have been to look for systems which could really make a difference, by using new technologies which are often already in use by different industries.
Furthermore the analysis misses out on assessing the potential impact of enhancing public awareness and actively engaging EU citizens, better field inspection methodologies and control, and the impact of strengthened law enforcement. How will the described Options either help or not in these areas?
Modern technology solutions could help combat counterfeiting and illicit trade. It requires the EU to go beyond what most Member States have been doing until now, and suggest the way forward is to evaluate the available new technologies. We therefore believe this study is a missed opportunity.
For example, taggant technology systems have a low implementation cost since it is integrated into the pack, while it reduces the risk for counterfeiting and fraud. Certain manufacturers and distributors have already installed this technology and are using it, providing potential economies of reusing this existing system. This has unfortunately not been considered in the analysis.

The costs related to Option 4 under 11.2.3 seem underestimated: based on the relevant experience of Atos syncing 2 separate solutions (one for printing and one for verifying) will lead to substantially higher implementing and operating costs.
Based on conversations with different Member States, we see as well that the Total Cost Of Ownership (TCO) linked to the use of tax stamps is generally underestimated (cost of transportation and storage, risk management of counterfeit,…)
Given the missed opportunity for studying the above described benefits, the costs and calculations as presented in 11.3.2 may be academic but bear limited value. We do not have insight on the modeling techniques and assumptions which have been mentioned under Section 11. Without this info it is not possible to provide further comments on Section 11.3.2.

D.2.

We recommend the use of GTIN and serial number as the unique code for the individual product/SKU level, and SGTIN for other packaging levels. For generation of a serialized Unique Identifier, we recommend a highly secure algorithm which takes into consideration the manufacturer, the individual product (SKU), based on a high level of randomization.

D.5.

We believe both machine and human readable codes are required:
A human readable code allows for every consumer to be involved in the process of verifying the authenticity of the product. It can also serve as a backup solution in case the machine readable code can't be read.
A machine readable code will help authorities to efficiently perform verifications. A machine readable code is essential during the manufacturing process, as a human readable code would not be able to support the printing at production speeds. A machine readable code is equally suited to support the aggregation process, which is at the heart of any effective track and trace offering. Machine readable codes could also be used by consumers with a smartphone, eliminating the risk of misreading the human readable code. A Covert Machine readable code also allows to include more information in the coding.

D.11.

We refer to our earlier remark that the feasibility study is only focused on assessing traditional 'paper based' security feature technologies. The report fails to assess alternative methods such as tear tape embedded with security features (which is used in many countries to carry covert, overt and forensic authentication technologies). Main advantage of this type of security feature is that it becomes an integral part of the existing packaging specification. This would reduce the impact and costs in terms of additional infrastructure requirements, and would be an alternative to the costly paper tax stamps, which are known to be easily copied or stolen.

D.13.

Based on the experience and expertise from Atos in the domain of Data management and storage, and reflecting on the requirements as described in Article 15 (8) of TPD, we point out the following important pillars related to Integration services & IT Security:

Integration services

To ensure an easy integration with the external world, the usage of proven market standards is for the envisaged system is important:

- Products are identified by an electronic Product Code (EPC)
- the specification EPCIS (Electronic Product Code Services Information Services) aiming to enable disparate applications to leverage Electronic Product Code (EPC) data via EPC-related data sharing, both within and across (enterprise and government) systems
- pack related information is stored in a machine readable code

From a technological point of view, the solution should be based on Service-Oriented Architecture concepts and provide external interfaces using well-accepted standards (Web Services, WSDL, SOAP) and wide-spread protocols (FTP, HTTP, HTTPS).

IT security : Measures to protect the system and its connections against threats from outside

Due to the amount and sensitivity of the manufacturing data, the system will have a special need for data protection and protection of the system itself, requiring the Data Management Provider to have an ample expertise in planning, implementing and operating security-critical systems.

In order to design an optimized protection the following activities typically need to be performed:

1. Analysis of protection requirement* with regard to the targets of confidentiality, integrity and availability
2. Implementation of an ISMS (Information Security Management System)
3. Implementation of the actual security systems (see listings below)

Step 1 will ensure that we plan for the necessary protection levels and do not overprotect certain areas while neglecting others. Results from the analysis will determine the implementation steps 2 and 3.

Step 2: The Information Security Management System (ISMS) describes all procedures and rules to control, maintain and improve IT-Security. It is absolutely crucial to maintain a consistent protection against the different types of threats. A proven and audited standard ISMS is vital, based upon which extensions and changes to this Standard would have to be implemented.

Step 3: The Technical Security Systems will enforce security rules and enable the automated detection of deviations. For the envisaged system in scope we consider the following security systems to be indispensable:

- Firewall/Proxy Services
- IAM – Identity and Access Management
- IDS/IPS – Intrusion Detection/Prevention System
- Full and strong Data Encryption for all data in transfer outside the datacenter
- Vulnerability Management Services
- Physical high security measures (Atos datacenter standard)

Additional technical systems/measures will be considered depending on the outcome of the protection requirements*:

- Web Application Firewall
- Data Encryption for data in storage, e.g. in the database
- Full and strong Data Encryption for data in transfer inside the datacenter
- DLP – Data Loss Prevention
- SIEM - Security Information and Event Management

- Security Operations Center to handle events from DLP and SIEM
- Strong Authentication by hardware-based digital certificates

In the design and the implementation of such Security Systems, we recommend to follow the relevant standards and all legal regulations (e.g. ISO 2700x). Moreover it is self-evident that in the course of the operations the security system will be audited internally and externally.

IT security : Measures to achieve a strict separation of access to the data of different stakeholders

The ISMS and its technical measures also ensure the high protection levels within the system. Requirements for a strict separation of access to data from the manufacturers will be ensured by employing the following measures:

- Design Measures (the design of the system will enforce that accidental or intentional access violations either from stakeholders or privileged users cannot take place)
    1. Incorporating a robust cloud security assessment service into the analysis of the protection requirements
    2. Designing and implementing an Identity and Access Management
    3. Application architecture supporting multi-tenancy
    4. The business logic has to be built to support multi-tenancy
    5. Physical separation of the databases
    6. Data encryption services inside the data center
- Operations Measures (detecting deviations during operations)
    1. DLP -Data Loss Prevention
    2. SIEM -Security Information and Event Management
    3. SOC - Security Operations Center

D.15.

Both a) and b) could provide reporting and query tools. The provider of data storage services could perform the role of certified interface to the Member States authorities and serve as trusted entity, independent from the manufacturers.

We consider the development of reporting and query tools to be a key consideration for making the TPD a success. It is important to develop and provide to the relevant authorities and stakeholders a highly secured Analysis platform, delivering Preventive IT Systems. This platform would provide advanced analytical capabilities, like anomaly detection, predictive analytics and advanced pattern recognition and would be supported by experts with in-depth vertical domain know-how, paired with advanced analytics skills.

Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective.
This platform would be based on handling different types of information flows consisting of structured and unstructured data, which will, by means of data mining and analytics, lead to useful information.
The main benefits and outcome would be useful information to be used by the relevant authorities for

- ► Spotting and predicting illicit trade patterns
- ► Focusing on critical cases and “big fishes”
- ► Improving efficiency and effectiveness for Law Enforcement

► Improving collaboration with other entities

D.17.

Any proposed tracking and tracing solution for the TPD must have at its heart the ability to uniquely identify products. Unique identification is not only important for the product authentication purposes, but should also support an aggregation process, and build a relationship between different levels of packaging, which is already part of the traditional manufacturing practice.
Interoperability is another key feature. There is a wide choice of existing coding systems suppliers which are supporting manufacturers across the EU and globally, allowing for reuse of the equipment at line level and systems as a whole at governmental or factory level. It is therefore recommended that any adopted tracking and tracing solution for use with the TPD would facilitate the reuse, if compliant with Open Standards.
Allowing as many suppliers as possible to support manufacturers and governments is the only practical approach to gain a successful outcome.
The main items to effectively fight illicit trade: Collaboration between industries and organizations, sharing knowledge and leveraging best practices, promoting open standards and technical development, and leverage the use of new technologies.

The key considerations regarding the implementation of the Tobacco Products Directive from Atos are:

1. **Technology should be part of a broader strategy.** Track &Trace systems can assist authorities to fight the growing issue of illicit tobacco trade. Today's technologies provide substantial improvement opportunities, but should be part of a broader strategy that also includes other measures: effective cross-border data exchange, interactive inspections, intelligent analysis tools, and enforcement in the field.
   Conclusion: technology should be embedded in a broader strategy

2. **International co-operation and information exchange.** Illicit trade is a cross-border phenomenon. The TPD can only be effectively implemented if member states and their enforcement agencies can co-operate and exchange information. The technological consequence of the need for co-operation and exchange is the choice for open standards-based systems. Atos supports the use of GS1 standards to identify products, capture the information at key points in the supply chain and then share the information seamlessly among stakeholders. This approach will ensure:
   - Easy integration with and interoperability between existing governmental systems, enforcement agencies and even industry
   - The ability to work cross border and effectively fight illicit trade
   - Ability of governments to use standard smart-phones and scanning devices for in-field inspections. This reduces cost and complexity, and ensures easy system maintenance.
   - Dependence on one specific supplier or use of proprietary systems will not lead to cost and system efficiency, and will limit future innovation
   - Avoid a European patchwork of standards that will raise the cost and complexity and making an effective tobacco control impossible

   Conclusion: open standards-based systems allow international co-operation and information exchange.

3. **Co-operation with private sector.** We see two benefits of a basic co-operation between the authorities and the private sector, in relation to the implementation of the TPD.

- Many major tobacco suppliers already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats. That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.

The Atos Competence Centre was involved in relevant Authentication and Track &Trace projects, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.

Conclusion: A basic co-operation with affected industries allows government agencies, when implementing the TPD, to benefit from industry's systems, expertise and budgets.

4. **Preventive/ predictive systems** Combining repressive measures and preventive measures is highly effective. Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective. Preventive/predictive systems can be a key tool for different agencies involved in fighting back against illicit trade.
   Important structured data sources are:
   - Digital Track & Trace systems from product suppliers and/or governments: If such systems apply digital coding on the products on the level of the SSU (smallest sellable unit), they can gain a deep insight in the movements of legal and illegal goods in a country.
   - Consumers: Today's smartphone and App technology allow citizens to check the authenticity of a product they are about to purchase. Involving citizens will multiply the amount of data that can be fed into analytical systems.

   Technological conditions for such citizen involvement: digital coding of products on pack level, and the use open standards (Atos supports the use of GS-1 standards)

   Conclusion: the use of preventive/predictive analytical IT systems is highly effective to fight illicit trade, and should be stimulated.

Attachment D.17

EC Consultation – Atos written statements

Atos SE (Societas Europaea) is a leader in digital services with 2014 pro forma annual revenue of circa € 11 billion and 93,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. A trusted partner for governmental institutions in many European countries, Atos provide services in areas such as e-tax filing, defence/ intelligence/ security systems, electronic truck tolling, as well as intelligent electronic regulatory reporting systems.

Atos has set up a Global Centre of Competence Serialization that supports the local application of IT systems to effectively fight illicit trade. Through the Centre we have successfully implemented effective, IT based Product Authentication and Track & Trace solutions across several industries, from pharmaceutical to tobacco and luxury goods.

B.1.5.

Option 1: Option 1 provides several advantages compared to the other options. It is based on an outlined cooperation between the authorities and the private sector. Compared to the other options it allows for capturing industry key learnings and leveraging the existing methods and installed systems. The option is based on reusing the existing systems currently used by the industry. This increases feasibility and cost efficiency for all stakeholders. It also reduces system implementation lead time.
We see two key benefits of an outlined cooperation with the tobacco industry:

- Many different companies already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats.

That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.
The Atos Competence Centre was involved in relevant Authentication and Track & Trace projects in different industries, including tobacco, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.
It is imperative Option 1 is implemented and operated under stringent control and audit rules as defined and endorsed by the Authorities.

Option 2: While Option 2 could leverage the advantages related to an EU wide approach (i.e. leading to one harmonized system), we foresee serious issues with the technical and organizational feasibility of this scenario.
Given the EU market size of tobacco products and the related amount of events to be captured, the size and manageability of one EU data repository would be very challenging. Also the alignment of the member states is a complicating factor. We fear this will result in delays in implementation time and will

not lead to a user friendly system, with compromises on usability (ex. system response time) and functionality.
The suggestion in Section 8.3.1 'Key principles' to replicate data to the Member States will increase overall level of efforts, both for the involved Solution Providers and the Member States, and lead to a higher overall cost.
Section 8.3.1'Key principles' also states that the solution may be operated by one (or more) solution provider(s) implementing a community wide traceability system. It is likely this would in fact create a kind of monopoly position for this solution provider. The European and National authorities would become dependent on one single solution provider. This can have negative impact on the cost efficiency and will limit the dynamics of future innovation.
Option 2 therefor does not seem to be a very realistic scenario, as the alignment of all Member States and stakeholders will be challenging due to mentioned technical, economical, but also organizational inconveniences.

Option 3: This option would increase costs unnecessarily (cost of dbase replication), prevent economies of scale and is not a good basis for encouraging collaboration between Member States, which is a prime condition for effectively fighting illicit trade. Since the databases would be driven by the Member States, the exchange of information and view on the complete supply chain is becoming difficult. Moreover, it goes against the reality of illicit trade, which is for the largest part organized internationally, and is currently exploiting the inability of Member States to collaborate. It would also create substantial challenges for the manufacturers, who would need to abide several Member State defined solutions, with each solution potentially operated by a different solution provider. The chance is very likely that this Option will not achieve what it is supposed to be doing: reduce illicit trade.

Option 4:
In general terms we support the search for creating synergies by means of combining the traceability option with the security feature based upon integrating the Unique Identifier. A key condition to creating such a synergy is to opt for security features based on digital technologies.
Since all 4 suggested Options related to security features involve a paper based stamp in some format, this does not seem feasible: combining a 'digital' data carrier with a paper based security features will not lead to synergies. It will complicate matters, and create extra costs without providing value.
This Option demonstrates the main issue of how the study has been handled: It wrongly assumes that the only viable security features available today are 'traditional' technologies linked to paper stamps or banderoles. The study did not properly investigate the potential of digital alternatives. New technologies such as digital tax stamps or fingerprinting technology can provide a lot of advantages over paper based technologies.
Moreover, there is a lot of focus on the security features itself and less on the practicality of the proposed paper based security systems, which is a missed opportunity. Digital alternatives will support the activities from the stakeholders* fighting illicit trade a lot better, and will allow for better integration with T&T systems (*Customs, Tax Authorities, Border police, Criminal Police,…).
If not reevaluated, it will cause the current Option 4 to fail its purpose and not lead to the economies as described in Section 8.5 of the feasibility study.

B.2.5.

As a general comment we disagree with the report and analysis, which only focuses on traditional solutions, while not exploring innovative and new solutions. The potential benefits of technologies such

as digital stamps, fingerprint of the products pack or fingerprint of the authorized printers should have been analyzed in the report.
Instead, the report only focused on exploring security features based on paper-based stamps or labels, and suggesting in all 4 options that paper stamps are needed. These are often counterfeited and create a false sense of security, as it may only provide information about the label itself, not the product. The ambition of TPD, and what it is trying to achieve, requires the use of advanced technologies which enable the authentication of products based on the individual physical properties of the product. A key success factor will be the ability to provide authentication of the pack, not a stamp or a label. It is therefore important that the Commission orients itself to embracing and promoting new technologies.

C.1.1.

The feasibility study has only focused on assessing traditional 'paper based' security feature technologies. As referred to in Section 8.5.1 'Key Principles' of Tobacco Traceability Option 4, this is the key building block you could integrate with the 'digital' traceability solution to explore synergies. We refer to our relevant remarks under Section 4 in B.1.5 of this document, in which we state that the combination of a 'digital' data carrier with a paper based security features will not lead to synergies. We therefor suggest that 'digital' alternatives are properly evaluated in a follow up study.
The study fails to reflect on the practicality of the different Options, and how some of the key stakeholders* would benefit from the systems, or not (*Customs, Tax Authorities, Border police, Criminal Police who focus on fighting illicit trade). We are convinced that in case new technologies would have been considered, the benefit analysis would be substantially better. The current benefit analysis as described in Section 11.3 is simply generic and fails to provide tangible value to the Commission and the EU MS.
We agree with the finding of the report under Section 11.3.1 'Benefit Analysis' that it is likely that any combination of the 4 solution options will provide 'similar' results. We think however this result will be mediocre to poor in case new technologies are not adequately considered. We think this would be a missed opportunity. For example: the described 'traditional' tax stamps and overt security features have been around for many years but have not proved very successful for goods identification and fighting illicit trade. They are found to be copied easily, or removed from a legal pack to be used on smuggled products or counterfeited. The ambition of this feasibility study could have been to look for systems which could really make a difference, by using new technologies which are often already in use by different industries.
Furthermore the analysis misses out on assessing the potential impact of enhancing public awareness and actively engaging EU citizens, better field inspection methodologies and control, and the impact of strengthened law enforcement. How will the described Options either help or not in these areas?
Modern technology solutions could help combat counterfeiting and illicit trade. It requires the EU to go beyond what most Member States have been doing until now, and suggest the way forward is to evaluate the available new technologies. We therefore believe this study is a missed opportunity.
For example, taggant technology systems have a low implementation cost since it is integrated into the pack, while it reduces the risk for counterfeiting and fraud. Certain manufacturers and distributors have already installed this technology and are using it, providing potential economies of reusing this existing system. This has unfortunately not been considered in the analysis.

The costs related to Option 4 under 11.2.3 seem underestimated: based on the relevant experience of Atos syncing 2 separate solutions (one for printing and one for verifying) will lead to substantially higher implementing and operating costs.
Based on conversations with different Member States, we see as well that the Total Cost Of Ownership (TCO) linked to the use of tax stamps is generally underestimated (cost of transportation and storage, risk management of counterfeit,…)
Given the missed opportunity for studying the above described benefits, the costs and calculations as presented in 11.3.2 may be academic but bear limited value. We do not have insight on the modeling techniques and assumptions which have been mentioned under Section 11. Without this info it is not possible to provide further comments on Section 11.3.2.

D.2.

We recommend the use of GTIN and serial number as the unique code for the individual product/SKU level, and SGTIN for other packaging levels. For generation of a serialized Unique Identifier, we recommend a highly secure algorithm which takes into consideration the manufacturer, the individual product (SKU), based on a high level of randomization.

D.5.

We believe both machine and human readable codes are required:
A human readable code allows for every consumer to be involved in the process of verifying the authenticity of the product. It can also serve as a backup solution in case the machine readable code can't be read.
A machine readable code will help authorities to efficiently perform verifications. A machine readable code is essential during the manufacturing process, as a human readable code would not be able to support the printing at production speeds. A machine readable code is equally suited to support the aggregation process, which is at the heart of any effective track and trace offering. Machine readable codes could also be used by consumers with a smartphone, eliminating the risk of misreading the human readable code. A Covert Machine readable code also allows to include more information in the coding.

D.11.

We refer to our earlier remark that the feasibility study is only focused on assessing traditional 'paper based' security feature technologies. The report fails to assess alternative methods such as tear tape embedded with security features (which is used in many countries to carry covert, overt and forensic authentication technologies). Main advantage of this type of security feature is that it becomes an integral part of the existing packaging specification. This would reduce the impact and costs in terms of additional infrastructure requirements, and would be an alternative to the costly paper tax stamps, which are known to be easily copied or stolen.

D.13.

Based on the experience and expertise from Atos in the domain of Data management and storage, and reflecting on the requirements as described in Article 15 (8) of TPD, we point out the following important pillars related to Integration services & IT Security:

Integration services

To ensure an easy integration with the external world, the usage of proven market standards is for the envisaged system is important:

- Products are identified by an electronic Product Code (EPC)
- the specification EPCIS (Electronic Product Code Services Information Services) aiming to enable disparate applications to leverage Electronic Product Code (EPC) data via EPC-related data sharing, both within and across (enterprise and government) systems
- pack related information is stored in a machine readable code

From a technological point of view, the solution should be based on Service-Oriented Architecture concepts and provide external interfaces using well-accepted standards (Web Services, WSDL, SOAP) and wide-spread protocols (FTP, HTTP, HTTPS).

IT security : Measures to protect the system and its connections against threats from outside

Due to the amount and sensitivity of the manufacturing data, the system will have a special need for data protection and protection of the system itself, requiring the Data Management Provider to have an ample expertise in planning, implementing and operating security-critical systems.

In order to design an optimized protection the following activities typically need to be performed:

1. Analysis of protection requirement* with regard to the targets of confidentiality, integrity and availability
2. Implementation of an ISMS (Information Security Management System)
3. Implementation of the actual security systems (see listings below)

Step 1 will ensure that we plan for the necessary protection levels and do not overprotect certain areas while neglecting others. Results from the analysis will determine the implementation steps 2 and 3.

Step 2: The Information Security Management System (ISMS) describes all procedures and rules to control, maintain and improve IT-Security. It is absolutely crucial to maintain a consistent protection against the different types of threats. A proven and audited standard ISMS is vital, based upon which extensions and changes to this Standard would have to be implemented.

Step 3: The Technical Security Systems will enforce security rules and enable the automated detection of deviations. For the envisaged system in scope we consider the following security systems to be indispensable:

- Firewall/Proxy Services
- IAM – Identity and Access Management
- IDS/IPS – Intrusion Detection/Prevention System
- Full and strong Data Encryption for all data in transfer outside the datacenter
- Vulnerability Management Services
- Physical high security measures (Atos datacenter standard)

Additional technical systems/measures will be considered depending on the outcome of the protection requirements*:

- Web Application Firewall
- Data Encryption for data in storage, e.g. in the database
- Full and strong Data Encryption for data in transfer inside the datacenter
- DLP – Data Loss Prevention
- SIEM - Security Information and Event Management

- Security Operations Center to handle events from DLP and SIEM
- Strong Authentication by hardware-based digital certificates

In the design and the implementation of such Security Systems, we recommend to follow the relevant standards and all legal regulations (e.g. ISO 2700x). Moreover it is self-evident that in the course of the operations the security system will be audited internally and externally.

IT security : Measures to achieve a strict separation of access to the data of different stakeholders

The ISMS and its technical measures also ensure the high protection levels within the system. Requirements for a strict separation of access to data from the manufacturers will be ensured by employing the following measures:

- Design Measures (the design of the system will enforce that accidental or intentional access violations either from stakeholders or privileged users cannot take place)
    1. Incorporating a robust cloud security assessment service into the analysis of the protection requirements
    2. Designing and implementing an Identity and Access Management
    3. Application architecture supporting multi-tenancy
    4. The business logic has to be built to support multi-tenancy
    5. Physical separation of the databases
    6. Data encryption services inside the data center
- Operations Measures (detecting deviations during operations)
    1. DLP -Data Loss Prevention
    2. SIEM -Security Information and Event Management
    3. SOC - Security Operations Center

D.15.

Both a) and b) could provide reporting and query tools. The provider of data storage services could perform the role of certified interface to the Member States authorities and serve as trusted entity, independent from the manufacturers.

We consider the development of reporting and query tools to be a key consideration for making the TPD a success. It is important to develop and provide to the relevant authorities and stakeholders a highly secured Analysis platform, delivering Preventive IT Systems. This platform would provide advanced analytical capabilities, like anomaly detection, predictive analytics and advanced pattern recognition and would be supported by experts with in-depth vertical domain know-how, paired with advanced analytics skills.

Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective.
This platform would be based on handling different types of information flows consisting of structured and unstructured data, which will, by means of data mining and analytics, lead to useful information.
The main benefits and outcome would be useful information to be used by the relevant authorities for

- ► Spotting and predicting illicit trade patterns
- ► Focusing on critical cases and “big fishes”
- ► Improving efficiency and effectiveness for Law Enforcement

► Improving collaboration with other entities

D.17.

Any proposed tracking and tracing solution for the TPD must have at its heart the ability to uniquely identify products. Unique identification is not only important for the product authentication purposes, but should also support an aggregation process, and build a relationship between different levels of packaging, which is already part of the traditional manufacturing practice.
Interoperability is another key feature. There is a wide choice of existing coding systems suppliers which are supporting manufacturers across the EU and globally, allowing for reuse of the equipment at line level and systems as a whole at governmental or factory level. It is therefore recommended that any adopted tracking and tracing solution for use with the TPD would facilitate the reuse, if compliant with Open Standards.
Allowing as many suppliers as possible to support manufacturers and governments is the only practical approach to gain a successful outcome.
The main items to effectively fight illicit trade: Collaboration between industries and organizations, sharing knowledge and leveraging best practices, promoting open standards and technical development, and leverage the use of new technologies.

The key considerations regarding the implementation of the Tobacco Products Directive from Atos are:

1. **Technology should be part of a broader strategy.** Track &Trace systems can assist authorities to fight the growing issue of illicit tobacco trade. Today's technologies provide substantial improvement opportunities, but should be part of a broader strategy that also includes other measures: effective cross-border data exchange, interactive inspections, intelligent analysis tools, and enforcement in the field.
   Conclusion: technology should be embedded in a broader strategy

2. **International co-operation and information exchange.** Illicit trade is a cross-border phenomenon. The TPD can only be effectively implemented if member states and their enforcement agencies can co-operate and exchange information. The technological consequence of the need for co-operation and exchange is the choice for open standards-based systems. Atos supports the use of GS1 standards to identify products, capture the information at key points in the supply chain and then share the information seamlessly among stakeholders. This approach will ensure:
   - Easy integration with and interoperability between existing governmental systems, enforcement agencies and even industry
   - The ability to work cross border and effectively fight illicit trade
   - Ability of governments to use standard smart-phones and scanning devices for in-field inspections. This reduces cost and complexity, and ensures easy system maintenance.
   - Dependence on one specific supplier or use of proprietary systems will not lead to cost and system efficiency, and will limit future innovation
   - Avoid a European patchwork of standards that will raise the cost and complexity and making an effective tobacco control impossible

   Conclusion: open standards-based systems allow international co-operation and information exchange.

3. **Co-operation with private sector.** We see two benefits of a basic co-operation between the authorities and the private sector, in relation to the implementation of the TPD.

- Many major tobacco suppliers already have existing Track & Trace systems in place which harbour a wealth of information on the movement of their legal goods.
- Companies faced with counterfeiting and illicit trade suffer considerable brand damage and revenue loss. They often dispose of deep expertise and experience to fight these threats. That's why basic co-operation and aligning efforts between product suppliers and governments can make the fight against illicit trade more effective.

The Atos Competence Centre was involved in relevant Authentication and Track &Trace projects, and experienced the positive impact of good alignment and co-operation between public and private stakeholders.

Conclusion: A basic co-operation with affected industries allows government agencies, when implementing the TPD, to benefit from industry's systems, expertise and budgets.

4. **Preventive/ predictive systems** Combining repressive measures and preventive measures is highly effective. Preventive IT systems can perform sophisticated analytics and combine multiple data sources to reveal illicit trade patterns and predict the likelihood of criminal events. The combination of structured data (coming from product suppliers and government sources) and unstructured data (internet searches or social media) is very effective. Preventive/predictive systems can be a key tool for different agencies involved in fighting back against illicit trade.
   Important structured data sources are:
   - Digital Track & Trace systems from product suppliers and/or governments: If such systems apply digital coding on the products on the level of the SSU (smallest sellable unit), they can gain a deep insight in the movements of legal and illegal goods in a country.
   - Consumers: Today's smartphone and App technology allow citizens to check the authenticity of a product they are about to purchase. Involving citizens will multiply the amount of data that can be fed into analytical systems.

   Technological conditions for such citizen involvement: digital coding of products on pack level, and the use open standards (Atos supports the use of GS-1 standards)

   Conclusion: the use of preventive/predictive analytical IT systems is highly effective to fight illicit trade, and should be stimulated.