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

```
AlpVision SA
████████████████
Rue du Clos 12
1800 Vevey
Switzerland
```

*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

```
350385813808-39
```

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

- **38791d0b-744c-4b17-bc36-1a1307cf9c45/CHE-109.076.493.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	○	○	○	●	○	○

5

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)

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	○	○	○	○	○	●

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)?

☐ 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.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)?

☐ 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.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;

☐ 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)

*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;
- ☐ 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

*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;
- ☑ c) A security feature is printed;
- ☐ d) A security feature is put on the pack/tin/puch/item through a different method;
- ☐ e) No opinion

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)

- **4e0c8c7f-4213-4b10-8138-9d11073348ad/Alpidrin_Packaging_Cryptoglyph_Authentication_Short.w**
- **1c1ae41a-0abb-4689-bb99-3ed7c47ed3f9/AlpVision_Tobacco_Packaging_Protection_A4.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)?

- ☐ a) A single centralised storage for all operators;
- ☐ 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)

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

- ☐ a) Provider of solutions to collect the data from the manufacturing and distribution chain;
- ☐ 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)

*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.b. If no, please explain your considerations

Text of 1 to 800 characters will be accepted

```
This would decrease the security of the whole system, giving critical
information to illicit trade actors that could use it for gray market or
counterfeit activities.
```

D.17. Please upload any additional comments on the subject of this consultation (max. 10 pages)
- **8508d452-6e97-4d40-835c-0700f7bc3258/EUTPD-20150724.pdf**

Contact

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

www.rc.vd.ch

Excerpt without cancellations

INTERNET EXCERPT

Ref. Nr   2001/06380
Fed. Nr   CH-550.1.025.213-9
UID/IDE CHE-109.076.493

Attachment A4

AlpVision SA
inscrite le 14 juin 2001
Société anonyme

Tobacco Packaging Protection

PROTECTION · ANTI-COUNTERFEITING · ADVANCEMENT · PATENTED · AUTHENTICATION

AlpVision's exclusive product authentication features

- **Non-intrusive, totally invisible**
- **No production changes**
- **No additional consumables**
- **Instant product authentication - no special reading devices required**
- **Highly secure**
- **Industry proven**
- **The best security/price ratio on the market**

AlpVision Cryptoglyph®

AlpVision Cryptoglyph® is a digital invisible marking that is applied to tobacco and cigarette packaging using regular visible ink and standard printing processes (offset, rotogravure, flexo, laser, inkjet, etc.).

Simple and industry-proven, AlpVision Cryptoglyph is ideal for large volumes and multi-plant deployment. It is commercialized worldwide under license agreements as an entirely customizable turnkey computerized system.

How it works

AlpVision Cryptoglyph is a digital image file that contains encrypted information. Integrated with prepress, the Cryptoglyph adds a pseudo-random pattern of invisible micro-holes (40 to 80 microns) into the standard varnish layer.

Cryptoglyph® integration

Non-intrusive and totally invisible, these micro-holes cover the entire surface of the packaging or label without changing its design.

Digitally encoded within the artwork, AlpVision Cryptoglyph can be easily integrated into any existing packaging or label printing process at zero production cost.

Highly secure, AlpVision's Cryptoglyph technology can only be deciphered with a 128-bit encryption key.
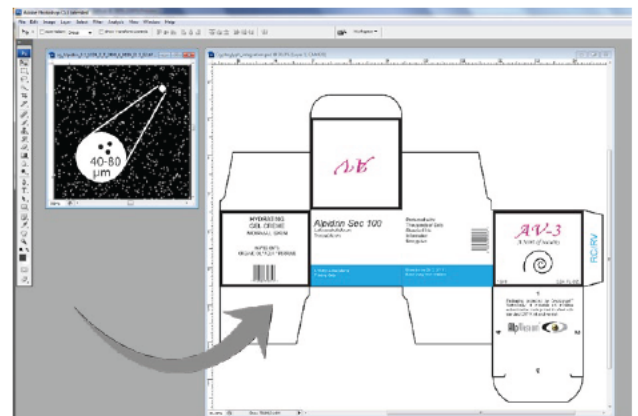
Non-intrusive and totally invisible, AlpVision Cryptoglyph is integrated into the packaging design.

1

Tobacco Packaging Protection

Detection devices

Unlike most covert anti-counterfeit features available on the market today, AlpVision Cryptoglyph does not require highly specialized equipment to be detected.

A standard office **scanner** can be used for a "genuine-or-fake" verification. For local authentication, install AlpVision's exclusive authentication application on your computer. For remote authentication, upload the scanned image to your secured server. Whether local or remote, the "genuine-or-fake" result will be displayed within seconds on your computer screen.

A regular **iPhone** equipped with AlpVision's custom product authentication application can also be used to verify the authenticity of a package. Working in real-time, verification usually takes less than 3 seconds, including time to pick up the package and position the iPhone over it. The application is also a powerful tool to perform market studies, announce product releases, promotional discounts, and upcoming news and events.

A standard **USB microscope** connected to a regular PC operating system can also be used to perform instant product authentication at a speed of 15 detections per second.
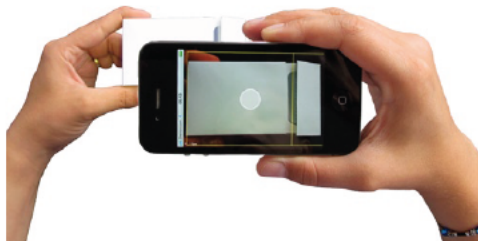

Tailor-made for large volumes and multi-plant deployment

As no additional consumables are required, AlpVision Cryptoglyph is especially well suited for large-volume, high-speed printing processes, such as rotogravure and flexography.

Turnkey solution

AlpVision provides an entirely customizable pre-configured turnkey solution that can either run on the client's own platforms or be hosted through AlpVision. As part of its standard services, AlpVision also provides staff training and support.

AlpVision®

To arrange an on-line demonstration
or for any further information, please contact us:

Address Rue du Clos 12 I 1800 Vevey I Switzerland
Telephone +41 21 948 64 64
E-mail avinfo@alpvision.com
Web www.alpvision.com

Address North American Regional Office I Sears Tower
233 South Wacker Dr., 84th Floor
Chicago, IL 60606 I USA
Telephone +1 312 283 8260
US Toll-Free +1 877 545 2121

EUTPD TECHNICAL REPORT COMMENT

AUTHENTICATION TECHNOLOGY FOR TOBACCO PACKAGING

July 24th 2015

Table of Contents

1. INTRODUCTION

The assessment of covert technologies for EUTPD includes several major mistakes. As a result, several critical conclusions of the report related to covert technologies are wrong. In the following we point out those errors and propose a modified version of the Table 30, titled "Summary of covert security features technologies" (which original version is listed in Annex for reference).

2. COMMENTS RELATED TO THE RANKING OF COVERT SECURITY FEATURES

The following comments are specifically related to the covert feature section:

1. P.136, about sentence: "requiring only adaptation of digital print processes". Digital printing is basically not used in the tobacco industry. We guess the author meant digital modifications of files used for generating rotogravure cylinders or flexo/offset plates.

2. P.136: Table, typo error: Cryptoglyph, not Cyrptoglyph.

3. P.136: Defense against imitation, we disagree on the rating given by the report:
   a. Latent image: Latent images require patterns and filters where finest details are always well larger than 20 um. As a result, the defense against imitation is very low. In the best case, it cannot exceed the level of polarizing ink, which has been rated **25%** in the same table.
   b. Digital watermark: The standard printed digital watermarking technology is a robust invisible information which is invisibly embedded in image data. By essence, this robust information will copy flawlessly and is therefore not a security feature at all (We assume the authors were not referring to semi-fragile digital watermarking which is not operational and still a topic of research nor to digital printing of fully variable watermark which is not possible for tobacco applications). Therefore the defense against imitation should be the same as any covert feature which is easily copied, like fluorescent, thermochromic, photochromic or conductive Inks which are set at 25% in the same table.
   c. Covert symbology: It seems that the naming of "Covert Symbology" has been created by the report authors, since it is unknown in the field of brand protection. More critical, all the information we could gather on this topic shows that the underlying concept is based on a specific decoding strategy (for instance using the error detection codes for embedding auxiliary data) of a visible marking. In practice, this means that this code has the same security against imitation than a QR-Code, it should therefore be set to the same security level which is 0%.

4. P.126: Prevalence of device, we disagree on the following:
   a. This definition ranks a lens or filter as a more accessible solution than smartphones, the goal being that several EU authorities may want to have the simplest access to the authentication tool. However, there are much more people with a smartphone in their pocket than a filter. Therefore, it seems reasonable to think that technologies using smartphone authentication should be ranked higher than those using filters or lenses.

5. P.136: Prevalence of device, microparticles:
   a. The prevalence is set to 100% for latent image. In consideration of the previous remark, it should at least not exceed 75%.
   b. The prevalence is set to 100% for microparticles. However, visualization of this feature requires an optical resolution of 1 micrometer or even higher. It is not realistic to consider that such an optical device can be considered as 100% prevalent. In the most optimistic view, device prevalence should be considered as similar to nanotext impressions which are ranked 75% in the same table.

6. P. 136: Affordability: The affordability of Cryptoglyph is listed as 75%. However, the production cost is strictly equal to Digital Watermark since in both cases there is no change in the production process or consumables. Therefore, it should also be evaluated to 100%.

7. P. 136: Table re-computation. The table including those modifications is listed below:

Security Feature	Defense against Imitation	Affordability	Ease of Training	Suitability for Enforcement	Prevalence of Device	Overall
Cryptoglyph	50%	100%	75%	50%	75%	70%
Latent Image	25%	100%	50%	75%	75%	65%
Digital Watermark	25%	100%	75%	50%	75%	65%
Metamerik Ink	50%	75%	50%	50%	100%	65%
Covert Symbology	0%	75%	75%	75%	75%	60%
Microparticles	75%	50%	50%	50%	75%	60%
NanoText	50%	50%	50%	75%	75%	60%
Hologram	75%	50%	25%	50%	75%	55%
Laser Taggants	75%	50%	75%	50%	25%	55%
Magnetic Ink	25%	75%	50%	50%	75%	55%
Polarising Ink	25%	25%	50%	50%	100%	50%

3. CONCLUSION

The Cryptoglyph technology has the best ranking among all the covert technologies listed in the report. Therefore, we think that all the Options using covert features should therefore explicitly recommend the Cryptoglyph solution.

The following modifications are suggested:

- Option 1: Level 3, "Laser or machine readable taggant" should be changed to "Cryptoglyph", p. 248, table 38.
- Option 2: Level 3, "Laser or machine readable taggant" should be changed to Cryptoglyph, p. 251, table 39.
- Option 4: Level 3, "Laser or machine readable taggant" should be changed to Cryptoglyph, p. 257, table 41.

4. ANNEX

Original Table

Security Feature	Defense against Imitation	Affordability	Ease of Training	Suitability for Enforcement	Prevalence of Device	Overall
Covert Symbology	50%	75%	75%	75%	75%	70%
Cryptoglyph	50%	100%	75%	50%	75%	70%
Latent Image	25%	100%	50%	75%	75%	65%
Digital Watermark	25%	100%	75%	50%	75%	65%
Metamerik Ink	50%	75%	50%	50%	100%	65%
Microparticles	75%	50%	50%	50%	75%	60%
NanoText	50%	50%	50%	75%	75%	60%
Hologram	75%	50%	25%	50%	75%	55%
Laser Taggants	75%	50%	75%	50%	25%	55%
Magnetic Ink	25%	75%	50%	50%	75%	55%
Polarising Ink	25%	25%	50%	50%	100%	50%