Annexure B: Security Feature Criteria and Assessment Findings

Reference: *European Commission: 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 – Interim Report I*

6.6 SECURITY FEATURES EVALUATION CRITERIA AND SUB-CRITERION

The domain of security features is complicated by the vast variety of different participants involved in the industry, as well as the relationships and interdependencies established between those operators. Some of these security printers have been in operation for several centuries, offering a broad menu of security feature options, whilst in some cases a specific security feature element is synonymous with the company itself, and requires closely guarded partnerships and alliances with other solution providers to supplement and create a more complete security feature product.
It is therefore not uncommon for security elements to be “mixed-and-matched” to develop a security package. Therefore, an analysis that focussed purely on the assessment of solution providers, would omit potential or emerging security feature technologies that potentially were not the purview of a solution provider. At the same time, regarding only the merits of a security feature technology, without consideration for the production, delivery and other operational aspects is also flawed. Therefore, to try and address these two considerations, the analysis for security features was conducted at two levels:

- An assessment of the solution providers themselves, using the Assessment matrix, modified to include assessment criteria derived from the security feature critical success factors derived from the problem statement in Section 2; and
- An evaluation of the security feature technologies, using the subset of assessment criteria developed for the Security Feature Assessment Matrix relevant to the technology itself.

In order to understand and rate each evaluation criteria effectively it was required to further distil each into sub-criterion. These criterions represented the level of detail against which each security solution provider was evaluated. The criteria and evaluation factors were prepared with reference to the Problem Statement and Security Feature Solution Critical Success Factors identified in **Error! Reference source not found.** in Section 2.3.2.

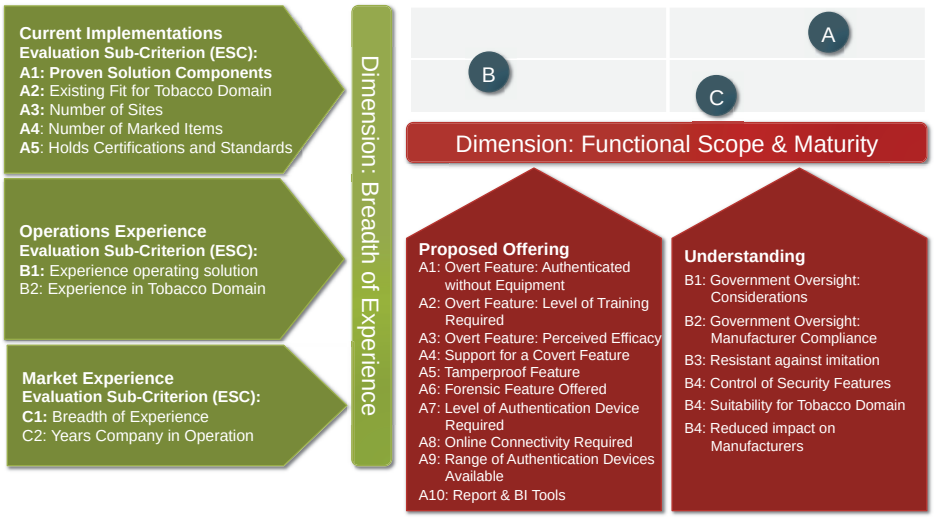

Figure 6 – Security Features Evaluation Sub-criterion

6.6.1 SECURITY FEATURES: FUNCTIONAL SCOPE & MATURITY

The functional scope & maturity axis consists of two primary dimensions: 1) The proposed offering of the solution provider, and 2) Level of understanding.

SECURITY FEATURE - DIMENSION: Functional Scope & Maturity		
Sub-Criterion (Weight)		**Description**
Criteria: A. Proposed Offering (Weight: 2)		
A1: Overt Feature: Authenticated without Equipment	3	▪ Does the overt feature meet the strict definition in terms of whether the cover feature can be authenticated without the support of an additional device or piece of equipment? ▪ Incorporated as such as a bridging mechanism to accommodate the requirements from TPD that specifies “visible”.
A2: Overt Feature: Level of Training Required	2	▪ Perceived level of communication and training that would be required to understand the authentication process and interpret the authentication result. ▪ Considered from the perspective of consumers as the primary users of the overt / visible feature.
A3: Overt Feature: Perceived Efficacy	2	▪ Consideration of how clear, verifiable and unambiguous the authentication result (from the perspective of the Consumer.
A4: Support for a Covert Feature	3	▪ A check that the solution provider is able to offer a security feature that includes a covert (hidden) authentication element.
A5: Tamperproof Feature	3	▪ Considers whether the solution provider offers elements to provide tamper resistance to the authentication feature.
A6: Forensic Feature Offered	3	▪ Tests whether the solution provider recognises the need to add the third component of a security feature package that includes forensic to the security package.

SECURITY FEATURE - DIMENSION: Functional Scope & Maturity		
Sub-Criterion (Weight)		**Description**
A7: Level of Authentication Device Required	2	▪ Considers the complexity and prevalence of devices that can be used to authenticate the covert security element. ▪ The EU problem statement and resulting functional requirements identifies several EU authorities that may be responsible for compliance monitoring and enforcement. The assumption is therefore that simple (e.g. a cheap polarising filter), common and multipurpose devices (e.g. smartphone) can increase reach and likelihood that the device will be on hand for field operations when required. ▪ Where the solution provider offers a range of authentication devices for multiple stakeholders, the best scoring devices rating is applied for this criterion.
A8: Online Connectivity Required	2	▪ Evaluates whether an online connection (to the Internet) is required during the authentication process. ▪ The requirement for online connectivity can impose some restrictions on where items can be authenticated, and this limitation may be a consideration for enforcement operations or market surveillance teams.
A9: Range of Authentication Devices Available	1	▪ Considers the extent the solution provider recognises the needs of different stakeholders (e.g. different use cases, affordability and degrees of authentication certainty), and is able to offer a range of authentication devices with different feature sets.
A10: Report & BI Tools	1	▪ Description of the available reporting tools and or data management components of the solution.
Criteria: B. Understanding (Weighting: 3)		
B1: Government Oversight: Considerations	1½	

SECURITY FEATURE - DIMENSION: Functional Scope & Maturity		
Sub-Criterion (Weight)		**Description**
B2: Government Oversight: Manufacturer Compliance	1½	▪ Recognises the requirement for a tobacco control solution that offers functions to aid oversight of tobacco manufacturing operations for EU authorities and understands these resources are precious. ▪ Support can extend to include reconciliation services and offering oversight of manufacturers to identify and alert anomalous events
B3: Resistant against imitation	3	▪ An evaluation of the team of the plausibility and degree to which the security feature and authentication result can be imitated. ▪ Note: This criterion considers **imitation**, and not duplication or counterfeiting of the overt security feature. In other words, considers the extent to which the security feature can be imitated to the extent of falsely convincing a reasonable member of the public.
B4: Control of Security Features	3	▪ The security feature solution provider should have an established process for order and secure delivery of the security feature materials to manufacturers.
B5: Suitability for Tobacco Domain	3	▪ Method of application of security feature should be compatible with tobacco packs and tobacco production processes. ▪ Security feature solution should accommodate manufacturers that may be located outside of the EU. ▪ Security feature should accommodate low-volume manufacturers (different degrees of automation).
B6: Reduced impact on Manufacturers	2	▪ Equipment for application of security feature should be compatible with tobacco manufacturing lines. ▪ Consideration for minimising impact in terms of supplies and equipment maintenance.

SECTION 7.2.2 ASSESSMENT FINDINGS OF SECURITY FEATURE TECHNOLOGIES

The following section presents the analysis findings of the security technologies. The analysis considers the attributes and performance of the security feature technology and is therefore agnostic of any attributes or capabilities of the solution provider able to provide these security features.

Overt Security Features

The table below presents the findings of the assessment of the overt security feature technologies. For a description of the criteria used, please see 6.6.4

The analysis yielded the following preliminary findings:

- Colour shifting inks, various security printing techniques, foils and security threads were identified as a mix of competent security features. Colour shifting inks provided the highest

defence against imitation amongst this category. The assessment of films showed defence against imitation varied considerably with more expensive films providing better security.

- Holograms provided a mixed overall performance. Whilst basic holograms are cheap to manufacture, they are very easy to imitate, creating a false sense of assurance. While highly sophisticated holograms (such as E-Beam from Holoflex) can contain security features that are almost impossible to copy, they are substantially more expensive and require extensive training for consumers and inspectors to authenticate. Because of this, basic holograms are not considered to provide efficient overt security, but can embed very strong and proprietary covert security features.
- Several security features that are effective for currency protection or brand protection were identified as not suitable for tobacco products. To be irremovable, it would require that the security feature be placed under the clear wrap on the cigarette pack, which would prevent tactile feedback (for authentication of intaglio printing) and light transmission effects (such as holding up to a light to verify watermarks or security films).

Table 1 - Summary of Overt Security Feature Technologies

Security Feature	Defence against Imitation	Affordability	Ease of Training	Suitable for Tobacco Control	Overall
Colour Shifting Inks	◑	◑	◕	◕	◑
Printing: Guilloche	◔	◕	◑	◕	◑
Printing: Microprinting	◔	◕	◑	◕	◑
Security Threads and Fibres	◑	◑	◑	◑	◑
Other OVD – Films	◑	◔	◑	◕	◑
Iridescent ink	◔	◕	◑	◕	◑
Metallic Inks	○	●	◑	◕	◔
Hologram (datamat**rix)**	◔	◕	◔	◕	◔
Holograms (EBeam)	◕	○	○	◕	◔
Holograms (Stereogram)	◔	◕	◔	◕	◔
Hot and Cold Foil Stamping	◔	◑	◔	◕	◔
Watermarks	◔	◕	◕	○	◔
Holograms (2D/3D)	○	◕	◔	◕	◔
Printing: Intaglio	◑	◑	◑	○	◔

Covert Security Features

The table below presents the findings of the assessment of the covert security feature technologies. The preliminary analysis yielded the following findings:

- The analysis shows a wide spread of security features ranging from highly affordable semi-covert features, requiring a simple device such as a coin to authenticate, through to forensic isotopic taggants, highly secure but neither particularly affordable nor particularly suitable in the context of tobacco control.
- A number of covert technologies were identified as unsuitable for field officials inspecting tobacco products where using the authentication required damage to the tobacco packaging to access the security feature (e.g. coin reactive inks, thermochromic inks or chemical markers). Further, several required the addition of liquid substances to the security feature

for authentication testing (e.g. DNA taggants), making these less suitable for field enforcement and better suited as forensic features for laboratory analysis.

- In terms of affordability, latent images and digital watermarks were identified as the most affordable (requiring only adaptation of digital print processes), whilst RFID chips were identified as the most expensive.

Table 2 - Summary of Covert Security Feature Technologies

Security Feature	Defense against Imitation	Affordability	Ease of Training	Suitability for Enforcement	Prevalence of Device	Overall
Latent Image	◑	●	◑	◕	●	◑
Digital Watermarks	◕	●	◕	◑	◕	◑
Covert Symbology (Pagemark)	◑	◕	◕	◕	◕	◑
Microparticles (e.g.Charms)	◕	◑	◑	◑	●	◑
Metameric Ink	◑	◕	◑	◑	●	◑
Cyrptoglyph (Type of Watermark)	◑	◕	◕	◑	◕	◑
Nanotext (Nanoimpression)	◑	◑	◑	◕	◕	◑
Hologram (Covert features)	◕	◑	◔	◑	◕	◑
Laser Taggants	◕	◑	◕	◑	◔	◑
Polarising Ink	◔	◔	◑	◑	●	◑
Magnetic Ink	◔	◕	◑	◑	◕	◑
Tag Spheres	◑	◑	◑	◑	◔	◔
Serialised Hologram (Meditag)	◑	◑	◑	◑	◔	◔
Forensic Markers	●	◕	◔	◔	○	◔
Bi-Flourescent Ink	◔	◕	◑	◑	◔	◔
Infrared Ink (Anti-Stokes)	◔	◕	◑	◑	◔	◔
Nano Taggants	●	◑	◕	○	◔	◔
Chemical Markers (Spottag, Datag)	●	◑	◕	○	◔	◔
Fluorescent Ink	◔	◕	◑	◑	◔	◔
Thermochromic Ink	◔	◕	◑	○	●	◔
Coin Reactive Ink	◔	◕	◑	○	◕	◔
Photochromic Ink	◔	◕	◑	◔	◔	◔
RFID*	●	○	●	◑	●	◔
Conductive Ink	◔	◕	◕	○	◕	◔
QR / Serial Codes	○	◑	◕	◑	◑	◔
Isotopic Taggants	●	○	○	○	○	○

***RFID costs are generally considered prohibitive for pack level (approx 15x higher than other Security elements)**

This wide range of covert features illustrates the possibility of selecting multiple features to build a security package that allows different features to be available to different stakeholders. For example:

- A latent image authenticated using a relatively affordable card filter could be provided to retailers or distribution chain operators as a means to authenticate products. This may be suitable for some Member States considering policies to hold retailers responsible if they are found dealing in illicit goods.

- A laser taggant could be included exclusively for use as an authentication method for EU officials as the means of verification of goods in the field.

- Forensic markers may be incorporated as random particles in the label substrate and only used for laboratory analysis for collecting evidence for case prosecution.

Emerging Fingerprinting Feature Technologies

To complete the assessment, analysis was also performed on several fingerprinting technologies that rely on identifying and recording certain chaometric events that cannot be replicated. This emerging field offers several interesting developments for covert security features.
The analysis of three of these referenced in the survey responses is included in the table below.

Table 3 - Summary of Emerging "Fingerprinting" Technologies

Security Feature	Defence against Imitation	Affordability	Ease of Training	Suitability for Enforcement	Prevalence of Device	Suitable for Tobacco Domain	Overall
Print Entropy (Systech, Schreiner)	●	◕	◕	◕	◕	◔	3.8
FibreTag (Proof Tag)	◕	◑	◕	◕	◕	◑	3.7
Signoptic (Arjowiggins)	●	◑	◑	◑	◔	◔	3.0

All three of these technologies require an electronic device to complete the authentication, making them suitable as covert security features only. However, as some mitigation, two of those evaluated could be authenticated using a smartphone (together with proprietary application), while the indications that the materials fingerprinting for Signoptic requires at least a smart phone with a proprietary lens adaptor accessory.
An area of some concern in evaluation these emerging technologies is the concern that these concepts will prove reliable and affordable operating at sufficient pace to support the high production speeds associated with the tobacco industry. Its therefore imperative the ability of these technologies to operate under these conditions is important.