Overview **Authentication Technologies**

With the availability of various authentication solutions, companies and Government authorities are facing problem in selection of a specific authentication solution as the adoption of any given solution is a complex question involving issues, amongst others, of cost, compatibility, feasibility and reliability, and there are divergent views on which technologies should be adopted and the timing for their adoption. While these solutions can sometimes add to the problem, the right selection, usage & implementation of authentication solutions helps companies and authorities to keep them one step ahead of counterfeiting. For the reason The Authentication Times team decided to start a series of article on Authentication Technoligies. This is the first article of this series giving an overview of authentication technologies to the reader, and this will be followed by detailed articles on anti-counterfeiting, anti-tampering and tracking and tracing.

Authentication:

With the increase in counterfeiting, Authentication technologies play an important role in supporting brand strategies, helping to reduce the risk of fraud by deterring criminals and enabling stakeholders to identify and track genuine product with fake one.

Today, there are various number of authentication technologies available in the market, although all these technologies are applied in the three main areas of

i) Anti-Counterfeiting
ii) Anti-Tampering, and
iii) Track and Trace

Anti-Counterfeiting:

The common feature of anti-counterfeiting technologies is that they are edrtremely difficult to be counterfeited. Consequently, they help in identifying a genuine product. Based on the authentication requirements, such technologies may consist of overt, covert and forensic features, or a mix thereof.

Anti-Tampering:

Such solutions are found more in the food and pharmaceutical industry where there is a need to protect a product from adulteration or replacement. An intact anti-tampering feature is the consumers' assurance that the contents are genuine and not tampered or adulterated.

Track and Trace:

Track and trace technologies use mass serialization to provide a unique identity to each SKU. The IT technology then allows to keep a watch on each SKU through customised software that allow an authorised user to track the movement of this SKU across the entire supply chain. Depending upon the authorization level, each user may also be able to access additional information pertaining to the product such as manufacturing date and factory, expiry date, the market such SKU is meant for etc.

All these technologies can be categorised as either overt, covert, forensic or digital.

Overt, Covert, Forensic or Digital

Overt: Overt technologies are authentication devices built into labels, documents and packaging which are visible to the user and show dynamic visual effects. Their main advantage is the fast and easy, on the spot, visual authentication where no

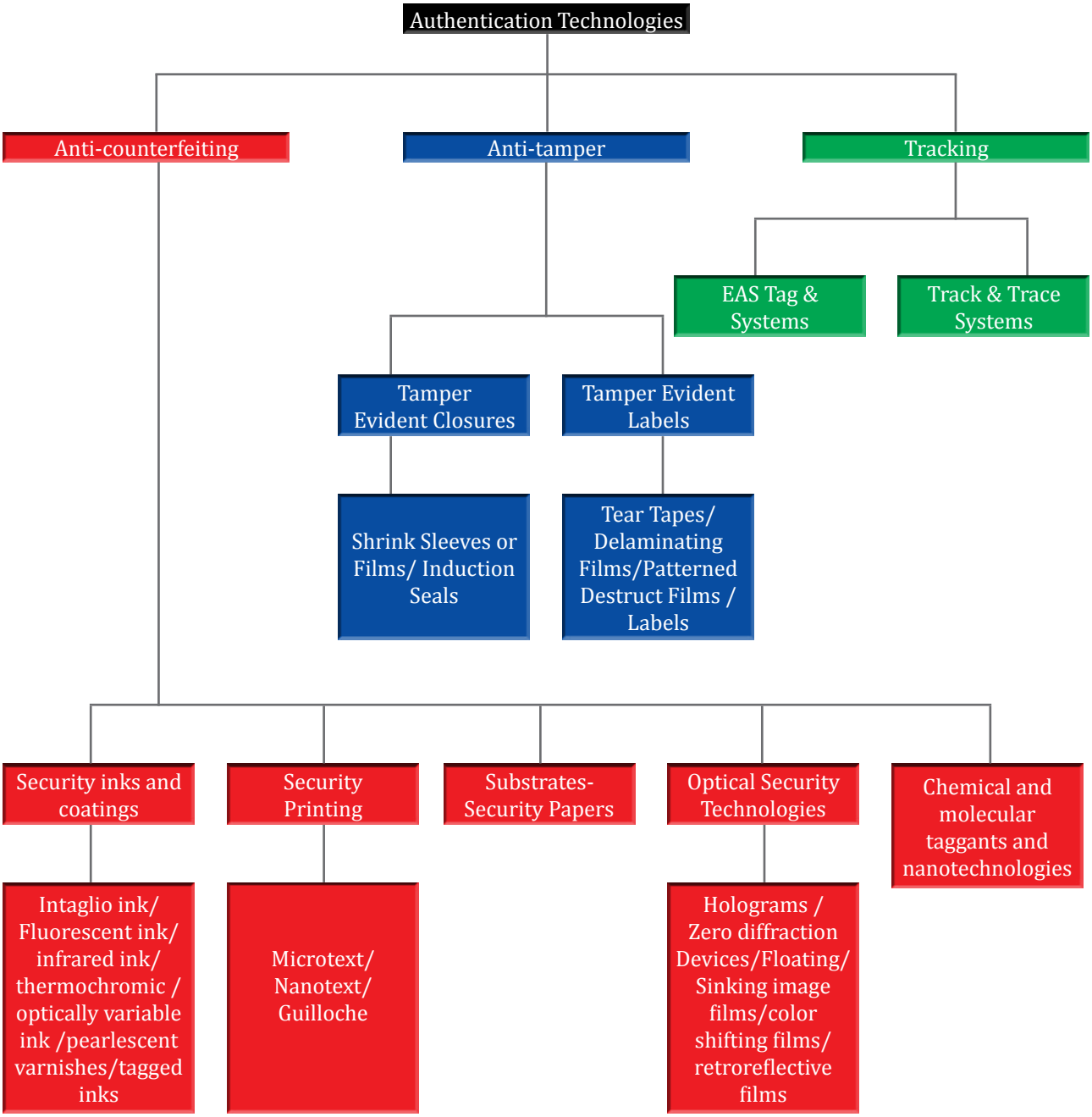

Fig: Diagram showing the primarily used authentication technologies

additional devices are needed. Overt features are expected to fulfil three main criteria;

- Communicate with the verifier
- Be easy to identify
- Be hard to copy and imitate

Physical secure solutions offering overt features include fine-line design, security guilloches, holograms, optically variable devices (OVDs), watermarks, colour-shift and thermochromic inks, threads, foils and laminates, embossable and laser markable films and security papers.

Overt features can be made more secure by combining them with covert, forensic and digital features. As Overt can be used for identification and verification by consumer, Covert *(Verification by a predetermined device or a tool)* can be used by manufacturer

Diagram: Overt feature (security hologram strip) applied on pharmaceutical product label

or their channel partner for an advanced level of authentication and verification. The third level is highly sophisticated and can be used by forensic experts and can be useful to law enforcement and for evidence in case of litigation. Mainly classified as overt technologies holograms produced in high security environment provide covert as well as forensic features.

Covert: Covert technologies are not instantly recognisable. They require a special reader or detector to be able to verify their presence and validity, and people using covert technologies will normally require some kind of training. Covert technologies include ultraviolet and infrared inks, micro text, unique synthetic tagging etc.

Forensic: Forensic technologies, being covert, are not readily recognisable and require special tools for detection and validation. Whereas covert technologies can be detected and validated in the field, forensic technologies must often be taken to a laboratory with specialised equipment.

Digital: Digital technologies may be either overt or covert, but all require an electronic means for detection and validation. Digital technologies are most associated with RFID tags or with serialised numbers that can be compared to a remote database.

Conclusion

In today's world when brand are under attack in forms of counterfeiting, tampering, pilfering, Authentication technologies play an important role in protecting brand reputation, value, market share and above all trust of customers. Counterfeiters target well known brands for illegal profit, which is further used to finance terrorist organization. Therefore, a product without authentication technologies represents a significant potential risk to society at large. There is no single solution to every problem, hence, a proper brand protection strategy involve combination of technologies with proper enforcement. It is pertinent to mention here ISO:12931 titled "Performance criteria for authentication solutions used to combat counterfeiting of material goods". This standard lays down some of the best practices to help brand owners to strategise and fight counterfeiting effectively. We believe that this tool should be adopted by all brand owners to eliminate counterfeit.

The next article will focus on anti-counterfeiting technologies in more details.