Protection Against Product Piracy

Sergej Toedtli at Vesdo Ltd looks at the implementation of product piracy protection infrastructures in large companies

The salesman has finished his presentation of a new, innovative authentication technology, which allows for the differentiation between counterfeit products from genuine ones. As he leaves the room, the discussion starts between the remaining attendants. The verdict is clear: it would be a promising technology for a single location factory; however, in the environment of a globally operating, multi-site group, it would be extremely difficult to implement and operate the system. In order to understand this statement better, I would like to outline the specific requirements of a large pharmaceutical manufacturer against the needs of a small company regarding the implementation of an infrastructure system to fight against product piracy.

DATABASE REQUIREMENTS

Without a specific anti-counterfeiting system in place, authentication is traditionally done by chemical analysis of the suspect sample, and the result is compared to the batch production data. This works fine, but it requires highly skilled personnel using expensive equipment, as well as being time-consuming and costly. By means of an authentication technology, an easy and instantaneous verification of the genuineness of a product is possible. Such authentication processes should be simple and therefore usable by a layman after little training. In such an authentication process, various properties and data of the primary and secondary package must be checked and verified. To do so, data are required, specifying the status of the genuine product. For example, the authenticating person must know what type of authentication feature has to be present on the inspected package carrying batch X and expiry date Y. To provide such data, a database is required.

This security database has to fulfil a multitude of tasks. As mentioned, its primary objective is to provide information to the authenticator. However, such a database is also an excellent repository for in-depth description of the various parameters of authentication features (for example, the hidden elements of a hologram), drawings and photos as well as training documentations. It allows the management of the life cycle of a security feature, such as tracking the deployment ramp-up. It also allows the centralisation of relevant data from various production sites and third party manufacturers in one repository, making authentication easy.

As we will see later on, the correct integration of security features is not an easy task. Therefore the first question of the authenticator in case of a missing feature will be: “Has the security technology been applied correctly?” It is also important to recall quality data of the security feature to make a plausibility check of the measured result.

Figure 1: Physical security feature, provided by Kodak. The taggants are embedded into the product material at very low concentration. Authenticity can be checked with a specific reader

There are not just internal users working with such a security database. In fact, suppliers of security features and packaging materials and even third-party packagers will have to access such a data repository from various locations, so internet access is mandatory. Secured access, as well as the management of user profiles and roles can be challenging. This database can be a part of the backbone business enterprise resource planning (ERP) systems such as Systems, Applications and Products (SAP) or a separate infrastructure. Both options provide a viable solution, but the use of an independent infrastructure is more common.

SECURED SUPPLY CHAIN

To secure packaging materials and products, two families of authentication technologies are in use: physical and logical security features.

Physical Security Features

These are substances or products which are introduced into or attached to packaging materials and products. For authentication, the presence of these security substances is checked. As the manufacturing process of security products is secret and its availability strictly limited, it is very difficult to counterfeit products secured in this way (see Figure 1).

Logical Security Features

These are based on encryption technologies, allowing the integration of hidden data into images and artworks (steganography, digital watermarks) and supporting the authentication of the product. It is also possible to register the surface structure features of a packaging material which are unique. With this data you can make an individual 'fingerprint' of each individual packaging item (see Figure 2).

In large companies, manufacturing and packaging are performed at a multitude of sites, with considerable volumes produced by independent third party suppliers. Packaging materials are mostly sourced from a multitude of local suppliers. Of course, the supply chain in such an environment is highly complex. If physical security substances or devices are used, the secured and controlled distribution from the security material manufacturer to all production locations and to the local packaging suppliers becomes a challenge. If such security substances or devices are diverted to counterfeiters, the criminals can produce 'genuine' products by using these illegally acquired security materials. To prevent such an incident, which would severely compromise the whole security infrastructure, sophisticated protection of the upstream supply chain for the security material is mandatory. Safeguarding precautions can include secure transportation and secure stocking, reconciliation processes and auditing. In short, a high degree of discipline in the supply chain is mandatory, which can be difficult to achieve, especially in view of the fact that quite often some or many logistical processes are outsourced.

Deploying logical security technologies can eliminate the headache of a secured supply chain as the security feature is sent as an encrypted data file directly to the print material supplier. However, other challenges must be overcome, as we will see.

QUALITY ASSURANCE

Logical security features are normally produced directly on the printing presses. During the pre-press activities, the printer integrates a security pattern or transforms print data through an encryption algorithm process. After printing, these security manipulations are very often invisible to the naked eye. To prevent illegal manipulation of secured packaging material, the encryption process allows for the introduction of information into the security patterns, allowing the identification of the packaging material manufacturer. Everything sounds perfect. So, where is the drawback?

To print logical security features, the printing process must be perfectly controlled and high-end print quality is required. This requirement concerns the whole printing process starting from pre-press, through plate making, to the printing press itself. It is recommended that manufacturing quality is permanently monitored by deploying specific test equipment. The bottom line is that logical security technologies cannot be given to any packaging material supplier. A careful selection and qualification of suppliers will be necessary.

As we have stated before, it can be of utmost importance to recall quality data at the point of authentication. To allow for this uploading of quality data into the secured database, the packaging material supplier will also need access to the data repository.

SECURITY

Regardless of the type of security technology in use, physical or logical, the trustworthiness of the packaging material supplier is a key requirement. However, whatever precaution has been taken, a certain risk will always remain. So the question will arise: 'is there a technology available for which these remaining risks are eliminated?' Indeed there is one, called 'material surface analysis'.

Most packaging materials do not have a smooth surface. Inspected under the microscope, fine surface structures resulting from the manufacturing processes are visible. As shown in Figure 3 (page 76), the wood fibres on carton surfaces can be seen. These fibre patterns are random, and cannot be reproduced. Therefore, an image of a defined area represents a unique fingerprint of the material which cannot be counterfeited. A further, very substantial advantage of this technology is the fact that no printing or application process is required: a simple scanning process is sufficient. Is this the silver bullet solution? Unfortunately not. This elegant method has two drawbacks. Firstly, the need to store significant volumes of data. Of course, the images are compressed and the fingerprint is a clever

Figure 2: Logical security feature, provided by Schreiner BitSecure. The printed security pattern contains information and cannot be copied

subset of the full data set. Nevertheless, a powerful database infrastructure is required.

The other shortcoming of this technology is the need for precise handling of the package in front of the camera. The exact location where the image of the surface has been taken must be known very precisely. Therefore in mass production, the image must be taken directly on the packaging line or at a specific coding station. This requires integrating a camera into the line, complemented by a data collection infrastructure. Such an expensive infrastructure does not normally pay off for surface structure registration alone. However, in combination with mass serialisation, it can be an attractive solution as both technologies can share the same infrastructure.

MASS SERIALISATION

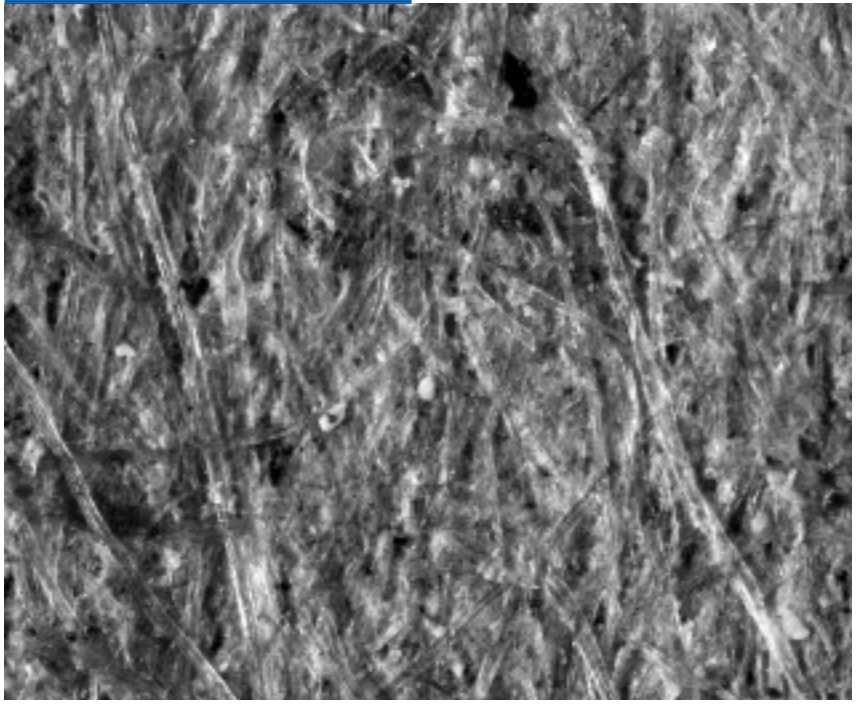
Mass serialisation is considered to be the backbone technology for protecting products against product piracy. There is no question that the combination of serialisation and traceability is an extremely useful countermeasure. It is effective against various forms of fraud, but the achievable level of security is somehow limited. Therefore, mass serialisation is most effective when combined with one of the authentication technologies as presented above. Serialisation and authentication technologies are complementary, and should be overlaid to provide optimal security.

Implementation of mass serialisation and traceability are mandated by many countries. Turkey has been the forerunner, and India has just published a law mandating serialisation. Similar legal requirements are expected from Brazil, Spain and China as well as from countries in the EU based on the EC legislative proposal relating to pharmaceutical packaging. The Data Matrix coding requirements in France, effective as of January 2010, necessitate the same technical infrastructures.

The barcode content as mandated by several legislations is unfortunately very heavy, requiring a Data Matrix barcode of up to 26x26 cells. On the other hand, real estate on the folding boxes is limited. Therefore, the codes have to be printed with an extremely high precision to guarantee sufficient barcode quality, which is important to ensure good readability. At the same time, coding must also be possible during the automated packaging process on fast running lines with speeds of up to 500 boxes per minute. To manage this development process, barcode quality assessment (verification) is of paramount importance. By deploying standardised and calibrated barcode verification instruments, the barcode quality level (grades) can be measured, allowing quantification of the success of the technical optimisation work for the serialising infrastructure.

One must also bear in mind that, for mass serialisation, a powerful database infrastructure is required. The question of whether this database should also support the operation of the authentication technologies, discussed in the first section of this article, is open to debate. Based on our experiences, we see that most companies currently deploy separate infrastructures to keep costs down.

Figure 3: Carton surface structure. The clearly visible fibres create a unique pattern for each carton surface and can be used for authentication



CONCLUSION

Implementing an infrastructure to fight product piracy in a globally operating pharmaceutical company is a demanding task. For the time being, there is no 'silver bullet' best practice solution available. For each and every company, a tailor-made solution has to be defined. The shortcomings of different technologies have to be compensated by combining them in order to provide effective protection against criminal attacks with a minimal impact on the cost of goods sold (COGS). As when constructing a building, a comprehensive architecture has to be prepared before starting. To develop such a concept successfully, considerable experience in the security industry is mandatory. As in most companies these projects have to be started from scratch and so the engagement of an external expert is highly recommended.

About the author

Sergej Toedtli holds a degree in Mechanical Engineering from the Federal Institute of Technology ETH in Zurich. After an extended career in executive management, he started his company, Vesdo Ltd, in 2000. As a security engineering company, Vesdo focuses exclusively on systems to protect its customers against product piracy. Email: toedtli@vesdo.com