

tesa scribos GmbH · Quickbornstrasse 24 · 20253 Hamburg, Germany

tesa scribos GmbH  
Office Address:  
Quickbornstrasse 24  
20253 Hamburg, Germany  
Telephone +49 40 4909-6330  
Telefax +49 40 4909-2670  
info@tesa-scribos.de

Via email:

Date 08.06.07

Your Ref./Your Letter

Our Ref.

Tel./Fax-Extension  
-4512

Contact E-mail  
joachim.suesse@tesa.com

We have structured our input along two main questions:

- under which circumstances is it possible to implement an electronic pedigree that enables the authentication of pharmaceutical products?
- which options exist and/or are required to alternatively or incrementally secure the pharmaceutical supply chain?

Your interest provided, it would be our pleasure to expand on the input given in more detail at your convenience.

### 1) Electronic pedigree

#### a) Mass serialization is prerequisite

In order to establish an electronic pedigree, each individual product needs to have its unique identity. This can be achieved by assigning an individual serial number or code to each individual pack.

#### b) Standardization of data structure is required

We agree to the statement of GS1 made in the workshop, that there is value in standardizing the data structure in which the individual product codes are being generated. In fact, it would be counterproductive in our view, if different structural models were to be imposed on the pharmaceutical supply chain as this would drive complexity and, hence, cost. This, in turn, would most likely lead to a lower

Commercial Register Heidelberg  
HRB 7200

ILN 43 99901 726611  
Registered office: Heidelberg

Directors: Dr. Christoph Dietrich, Peter Kuich  
Dr. Steffen Noehle, Joachim Suesse (Managing  
Director)

Dresdner Bank AG Heidelberg  
(BLZ 672 800 51), Nr. 4 800 114  
00  
VAT No. DE 813503237  
WEEE-Reg.-No. DE 16883776

level of compliance by the relevant stakeholders in the chain, coinciding with a lower level of acceptance and, consequently, hurdles in implementing any system effectively.

We also concur with the comparison made in the workshop which related to the development of today's standardized barcodes (e.g. EAN) used for virtually any product (though not on an individual level): it is difficult to conceive how cash registers in a supermarket (and the data bank connected to it) were supposed to function if the various suppliers were using different data structures in their barcodes.

c) Standardization of the data carrier is not required – 2D barcode is preferable

If the data structure is standardized, new technical developments of data storage systems can be implemented over time, depending on the benefits of a specific data carrier technology for the stakeholders in the supply chain.

Today, we see the 2D barcode as the technology best suited for mass serialization. Data storage capacity is sufficient to store even long individual codes, and the technology has been proven in the marketplace since many years with satisfying reading results. In addition – being in most cases based on printing technology – it is a very cost efficient means to assign an individual identity to the single product.

A 1D barcode does not compare well to the 2 D version due to data storage limitations and a rather high need for real estate on the product or package.

RFID - at its present development stage and for many years to come - is in our view not suited to fulfill the needs of the pharmaceutical supply chain for a variety of shortcomings: technical functionality (e.g. shielding by liquids or metal), lack of a standardization of operating wavelength, manipulation resistance, privacy, cost, etc. We concur with the assessment of Ed Dietrich from Reconnaissance International presented during the Global Forum succeeding the IMPACT workshop in Prague.

d) Application of data carrier onto the product is technically feasible

There are several options to apply a barcode to a pharmaceutical product, all of which can be realized without any major technical complications. Printing technologies, such as thermo-transfer or inkjet printing can be used for marking blister packs or cardboard/paper packaging material. Adhesive labels with the barcode printed on them can be applied within a standard automated labelling

process. Glass products such as vials or ampoules can be marked directly with laser-based inscription technologies (e.g. tesa laser transfer film technology). RFID modules can be easily attached to the product with adhesive technology.

e) Scope of pedigree needs to be determined – issues exist in all visible options

In our view, one of the major issues associated with a pedigree relates to the question as to whether the individual code can (or needs to) be retraced through all steps of the distribution chain – i.e. from manufacturer via all distribution steps to the pharmacy – or whether a manufacturer's code should only be verified at the point of dispensing, as proposed by EFPIA.

While a fully comprehensive system across all steps of the distribution chain would deliver highest level of transparency about previous whereabouts of any single product – and, hence, the highest level of security within any pedigree-based system – we see major obstacles in implementation. These are based on the presumably low level of interest of intermediate distribution layers (wholesalers, im-/exporters, secondary market players) in accepting the incremental burden of having to read/store/transmit the individual product codes which we deem to be without a perceived strong business value to them. In fact, there are most likely business interests of such distributors not to reveal sources or delivery destinations to their customers or the pharmaceutical manufacturers. In addition, the technical upgrade requirements to make all players in the supply chain capable of reading, checking, storing and/or transmitting the codes would be very significant and implementation would very likely be very time consuming. As a consequence, we see here a potential cause for substantial incremental cost as well as time delays and believe that an implementation of a full pedigree scope – should it be desired - would need to be supported by legislative means.

If product codes were only to be verified at the point of dispensing as proposed by EFPIA, there would be a lower degree of overall system security, as product movements between manufacturer and pharmacy are not traced, i.e. there would be a transparency gap. However, the key players of such a system - manufacturers and pharmacies - have a high interest in providing genuine product and are likely to support it, so that the risk associated with conflicting interests among key stakeholders is diminished. In the interest of a presumably shorter implementation duration, we would tend towards the solution approach suggested by EFPIA.

Implementation of the EFPIA proposal would obviously be less complex than the above encompassing approach, but not without significant technical challenges. The issue of establishing a central data bank (per country/region or even globally?) would need to be resolved so that pharmacists can check individual

product codes in one data bank rather than having to connect to a multitude of manufacturer data banks with different formats and access modes.

Next to technical complexities associated with establishing such data bank, the question of data ownership arises. In our opinion, this issue can best be addressed by having the system operated under the auspices of a neutral and trusted organization – we are not daring to propose WHO, although the idea comes to mind quickly.

A final major issue we see relates to parallel trade and associated repacking activities. As parallel trade is legal, and in some countries - such as Germany - certain import quotas are even mandated by the authorities, this distribution channel poses a risk for any type of authentication system. Repackaging and/or re-labelling of imported pharmaceuticals is done to comply with regulatory requirements of the country the drug is imported into. As a consequence, a product code may simply disappear if the drug is put into a new package so that the intended authentication becomes impossible.

As solution paths we can only visualize two options, both of which have major issues associated with them. The first is to mark the primary packaging (blister, vial, ampoule) with the same code as the secondary packaging (cardboard/paper), which is technically very demanding as codes need to be reliably matched within speedy and complex production processes.

The second option refers to regulatory means mandating the importer/re-packager to maintain the existence and integrity of security features, and we admit that we do not oversee the full legal and regulatory implications of this approach.

#### f) Pedigree-based authentication has limitations

The implementation of a pedigree-based authentication system would certainly improve security in the pharmaceutical supply chain, especially in developed countries where the basis for establishing a complex IT structure exists. However, we see three problem areas for which alternate and/or incremental protection measures are needed:

- in developing countries, the technical (IT) foundation to operate a comprehensive pedigree authentication system based on machine readable codes does only exist rudimentarily or not at all.
- with a pedigree-based system, merely (printed) codes are authenticated and not the physical properties of the pharmaceutical or its packaging. Printed barcodes are, however, easily counterfeited so that incremental protection of the code itself is advisable for products and/or geographies exhibiting a high risk of counterfeiting activity – preferably combined with a protective means that also serves to physically authenticate the pharmaceutical product.

- the stakeholder with the highest interest level in obtaining genuine products – the patient – would have essentially no means to authenticate his or her pharmaceutical product within a pedigree-based system building upon machine readable codes, so that overt security features are required if patient authentication is sought.

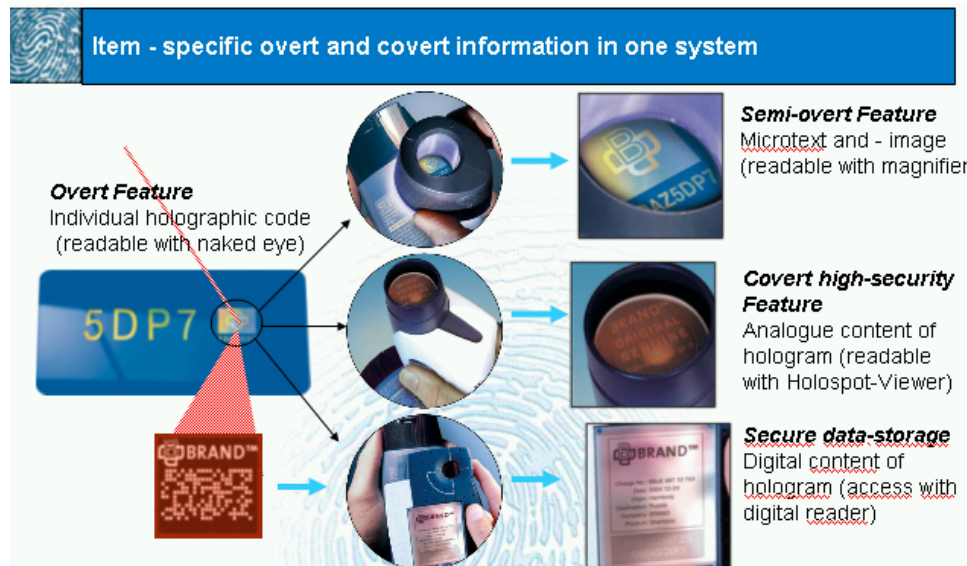
## 2) Alternate or incremental security options

We believe that all three problem areas mentioned above can be addressed with security technologies being on the market today as was elaborated upon during the WHO IMPACT workshop by various security providers including tesa scribos. The suggested solution path points at a multi-layer approach of combining selected overt and covert security features which can either be linked to a pedigree/coding system or not.

### a) Product protection without coding scheme

In developing countries with a lack of sufficient infrastructure to operate an authentication system based on machine-readable codes, overt features can serve as an authentication tool for the public (e.g. patients, pharmacists), while covert features can be utilized by authorities or other investigators in a “stand – alone” solution. Such an approach would obviously not have the benefits associated with a coding scheme.

Technically, high security technology can rather easily be implemented, for instance by applying small, so-called Holospot labels to a pharmaceutical package containing mass serialized individual holographic structures with overt and covert features to choose from:



## b) Product protection with human readable coding scheme

With the emerging growth of cell phone technology in developing countries, we subscribe to the notion presented in the workshop that cell phones represent a viable tool to support numbering/coding schemes for authentication in these parts of the world. As cell phone devices generally do not support the reading of digitalized 2 D barcode data, however, the use of human readable codes is suggested for authentication by the public. These codes can be generated by a security technology supplier (similar to the Meditag program in Malaysia) and be provided to a central (independent? government?) data bank so that certainty is achieved as to which codes are truly in circulation in any given country. Employing a call or SMS inquiry, a patient or pharmacist can then verify the code of the individual pharmaceutical product.

Merely printing or otherwise applying a human readable code on a product will in our opinion not suffice, though. As developing countries generally are exposed to a higher risk of counterfeiting activities as well as cell phone coverage is not encompassing enough to only rely on a coding scheme, it is additionally suggested to combine the human readable code with overt security features. This serves to establish a technological barrier towards code replication/counterfeiting while at the same time providing a means to authenticate any given product without the help of a cell phone. Semi-overt or covert security features can, of course, be employed for added security in this concept. The following example based on the tesa Holospot system may serve as a visualization of the proposed security feature combination on a self-adhesive label:

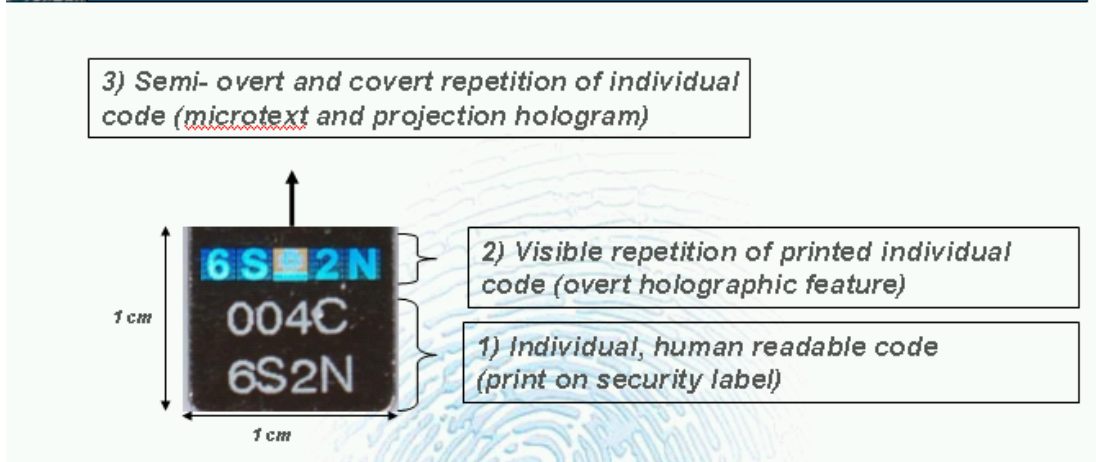
Commercial Register Heidelberg  
HRB 7200

ILN 43 99901 726611  
Registered office: Heidelberg

Directors: Dr. Christoph Dietrich, Peter Kuich  
Dr. Steffen Noehte, Joachim Suesse (Managing Director)

Dresdner Bank AG Heidelberg  
(BLZ 672 800 51), Nr. 4 800 114  
00  
VAT No. DE 813503237  
WEEE-Reg.-No. DE 16883776

**Example of a mass serialized, human readable code secured with Holospot technology**



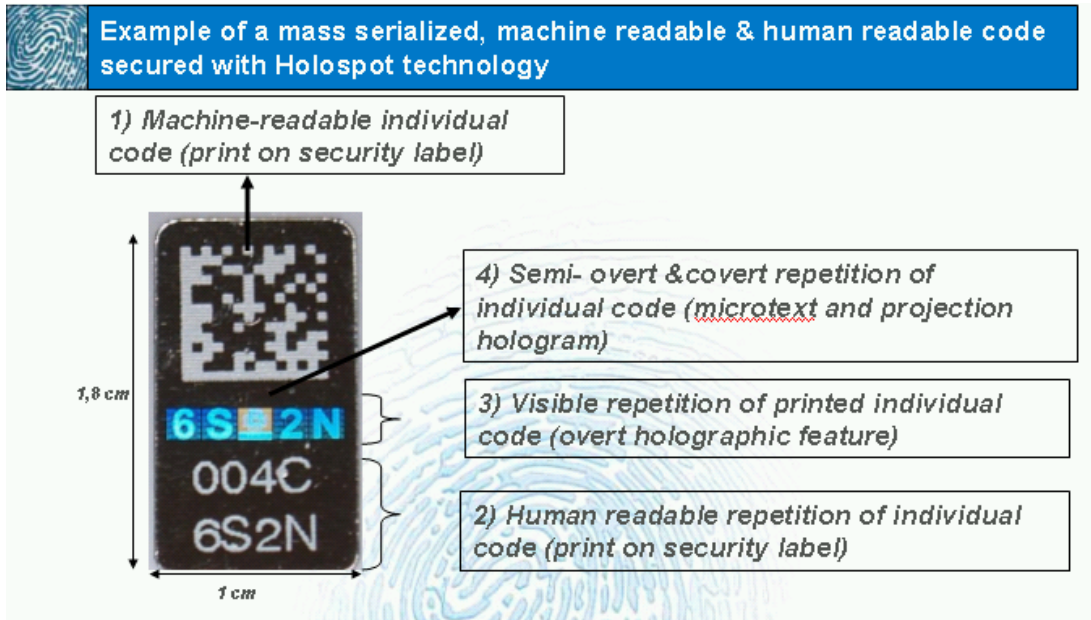
c) Product protection with machine readable and human readable coding scheme

For those country-specific environments in which a pedigree-based authentication utilizing machine-readable codes is technically conceivable, incremental security features can be implemented to protect selected pharmaceutical products especially susceptible to counterfeiting (e.g. see US NABP listing 2004 – attached).



List.pdf (28 KB)

Should patient authentication be a requirement in this scenario, again multi-layered overt and covert security features are a recommendable approach to product protection which can be even further enhanced by adding a corresponding human readable code for cell phone-based code verification. An example of a technical solution – again based on Holospot technology – is visualized in the following graph:



A multitude of authentication options does result from this feature combination:

- a web-based verification of the machine readable (2D) barcode or the human readable code (both to be identical),
- an authentication of the human readable code via cell phone,
- a authentication of the printed human readable code by matching it with the individual holographic code (to be identical in full or in part, e.g. last four digits in holographic format),
- a comparison of two individual packs can be made to compare the individual, visible holographic codes which need to be different from pack to pack,
- verification of the optical appearance (“rainbow effect”) of the visible holographic codes and micro text,
- cross-match of printed human readable code and semi-overt micro text code o be identical (magnifier required),
- the existence and the optical appearance of the projection hologram (special reading devices, specialists only),
- cross – match of printed, visible holographic as well micro text code with the code stored in the hidden projection hologram of the Holospot (specialists only – projection hologram may also contain additional security information as required).

Hence, the combination of logical (code-based) and physical (mass serialized holography) product protection systems adds up to a very high technological

barrier to counterfeiting. At the same time, public user friendliness and, consecutively, user compliance is likely to be enhanced by providing several, rather simple ways of authentication.

We hope that we could provide you with input that is valuable for your further considerations. Please do not hesitate to contact us if we can be of any further help to you. We would be glad to provide you with any additional information required for evaluating technological options or to support your endeavors in test or pilot projects.

Yours sincerely,

Joachim Suesse  
Managing Director  
tesa scribos GmbH