Comments and Consultation by UID systems and authentication providers Sanco.ddg1.d.3(2011)1342823

Inhalt

Introduction 2

About Securikett 2

About Kurz 3

About Brainority 3

About the Authors 4

Remarks on the Meaning of Safety Features vs. Unique Identifiers in the Directive 4

Securikett's Opinion on Unique Identifiers and whether they May be Considered as Safety Features, under a Cost Perspective 6

Thoughts about Exceptions from a Security Point of View 7

Proposing an Open Architecture for Unique Identifier Systems 8

UID systems are more than repositories 8

Gateways Make UIDs Systems Interoperable 10

Attribute Data Management Goes Beyond Simple Data Bases 11

Benefits of an Open Systems Architecture 11

What is a Format, what is a System – about the Relevance of GS1 "Standards" 12

Printing Format 12

Data Structure 13

What Does GS1 "Standard" Mean? 13

Systems as Opposed to Formats and Structures 13

How Can GS1 and an Open UID System's Architecture Be Linked Together? 14

Suggestion for a European Architecture 15

Steps to Realization: Feasibility Study by Running a Pilot 16

Some calculations on data to be stored and traffic to be handled. 16

Labels? About Benefits in Using Labels in the Context of the Directive 17

Tamper evident labels 17

Labels containing the UID 17

Questions Set in the Consultation 19

Consultation item n°1 19

Consultation item n°2 19
Consultation item n°3 19
Consultation item n°4 20
Consultation item n°5 20
Consultation item n°6 20
Consultation item n°7 21
Consultation item n°8 21
Consultation item n°9 22
Consultation item n°10 22
Consultation item n°11 23
Consultation item n°12 24
List of References 25

Introduction

This paper has been jointly developed by Dr. Marietta Ulrich-Horn, MBA, and Dr. Rainer Gerkens, representing the discussions and expertise of three companies

- Securikett Ulrich & Horn GmbH
- Leonhard Kurz Stiftung & Co.KG
- Brainority Software GmbH

By handing in this paper we are intending to contribute to an efficient implementation of the directive.

About Securikett

SECURIKETT®

The company is part of the long established Ulrich labels group. Ulrich has been founded in 1868 in Vienna and today is considered among the leading self adhesive label suppliers/manufacturers in Europe.

Drawing on this expertise, Securikett, which is a small-sized company according to the EU definition, has been founded in 2001 as a spin-off and devotes itself to the development and production of labels and related solutions to combat counterfeiting. As one of the leaders in tamper evident labels, Securikett is supplying such labels in large quantities, on a global base, to pharmaceutical customers, who make up for more than 50% of the company's annual sales. Securikett has also won several international awards in the area of tamper evident security labels.

Securikett also offers CODIKETT®, a highly secure web based system to create and manage unique identifiers with relations to the objects/packages they are assigned to, and to handle and issue the corresponding responses upon queries. This open architecture system allows for traceability and verification of items in the supply chain as well as at the point of sales.

Securikett is member of the IAA, the EAASM and the ACG.

Learn more about Securikett at www.securikett.com

About Kurz

The KURZ Group is a global leader in hot stamping and coating technology. KURZ develops and manufactures decorative and functional layers applied to carrier foils for a large variety of applications. With 3,800 employees in nine production plants in Europe, Asia and the USA, as well as 22 subsidiaries and 70 agencies around the globe, the KURZ Group manufactures and sells a comprehensive range of products for surface finishing, decoration, marking and counterfeit protection.

KINEGRAM® and TRUSTSEAL®, a host of diffractive optically-variable security features, today are in global use in the protection of governmental documents and banknotes as well as branded products such as pharmaceuticals.

KURZ also continuously invests in new technologies and has recently adopted SecuTrace®. By this open architecture web application, based on unique identifiers, KURZ rounds off its portfolio of extensive solutions for product and brand protection. The codes, in form of a 2D Datamatrix, may even be presented as part of a diffractive structure, to make it almost impossible to reprint or copy them.

Learn more about KURZ at www.kurz.de

About Brainority

The company's goal and expertise lies in protecting corporations' IT infrastructures and information assets against the risks of harmful software and hacking.

Brainority is the creator of CODIKETT®, the web based system, to deter counterfeits by creating and verifying unique identity codes.

Learn more at www.brainority.com

About the Authors

Dr. Marietta Ulrich-Horn, MBA is cofounder and manager of Securikett, where she is in particular in charge of R&D.

Being well acquainted with architecture and requirements of web based systems for identification on a single item level she is delegated by the Austrian Standards institute ASI as an expert in the ISO technical committee 247 WG3. The working draft WD16678 on "Guidelines for Interoperable Object Identification and Related Authentication Systems to Deter Counterfeiting and Illicit Trade" shall lead to an ISO Committee Draft within this year, and eventually to an international standard.

She is also delegated by ASI to ISO TC247 WG1, 16125, developing a standard on "Security Management Systems – Fraud Countermeasures and Control".

Further relevant for the realization of the directive is her work in CEN TC261, working on "Tamper Verification Features for Medicinal Packaging."

Dr. Rainer Gerkens holds a PhD in information technology from the University of Berlin and today is an expert in IT security. Drawing on his experience and expertise in this area, he is the program director of the UID system Codikett®, a system that can be used to deploy the requirements of the Directive. He also contributed to this paper by his suggestion of a layered architecture needed in this context.

Remarks on the Meaning of Safety Features vs. Unique Identifiers in the Directive

Paragraph 2 on page 2 of the consultation says:

"Directive 2011/62/EU introduces obligatory 'safety features' to allow, *inter alia*, verification of the authenticity of medicinal products ('unique identifier'). It places the Commission under an obligation delegated acts setting out the details relating to the unique identifier."

However reading Article 54a(2) of Directive 2001/83/EC, as amended by directive 2011/62/EU we read:

" the Commission shall adopt, by means of delegated acts ….., measures supplementing point (o) of Article 54 with the objective of establishing the detailed rules for the safety features referred to in point (o) of Article 54.

The delegated acts shall set out:

(a) The characteristics and technical specifications of the unique identifier of the safety features referred to in point (o) of Article 54 that enables the authenticity of medicinal products to be verified and individual packs to be identified. When establishing the safety features due consideration shall be given to their cost-effectiveness. …"

And to recall Article 54 (o):

" for medicinal products ….. safety features enabling wholesale distributors and persons authorised or entitled to supply medicinal products to the public to:

- Verify the authenticity of the medicinal product, and
- Identify individual packs,

As well as a device allowing verification of whether the outer packaging has been tampered with."

Comparing the statement in the Delegated Act Consultation with the Directive, it implies that the unique identifier as such shall be the only safety feature that will guarantee the authenticity of a medicinal product. It seems that by implementation of unique identifiers the question of product safety will be answered per se. This, to our opinion, is not the content of the Article 54(o), which mainly talks about safety features, authentication and (!) identification side by side.

Consulting the International ISO Standard 12931:2011 "Performance Criteria for Authentication Solutions in the Field of Material Goods" track & trace systems are explicitly excluded from authentication systems:

"Nor does this International Standard apply to technologies or systems designed for the tracking and tracing of material goods. Track and trace on its own is not an authentication solution and is therefore outside the scope of this International Standard."[1]

This exclusion, shared by most anti counterfeit experts, may sound harsh, but has to be understood against some possible pitfalls of unique identifiers:

- Data files of unique identifiers get stolen or compromised
- Creation system of unique identifiers gets cracked or compromised
- Codes are reprinted (cloning)
- Packages are opened and refilled with false medicine without notice
- Unauthorized producers, such as counterfeiters enter their own unique identifiers into the public system (under discussion in this consultation), without being noticed

[1] ISO Standard 12931:2011, page 1

Securikett's Opinion on Unique Identifiers and whether they May be Considered as Safety Features, under a Cost Perspective

To follow the Directive in its original sense, the unique identifier shall be combined with some other independent authentication feature. We believe this has been meant by "safety feature" in the wording of the Directive. Such features may be

a. Overt safety features
    i. Holographic
    ii. Colour shifting ink – the colour changes depending on viewing angle
    iii. UV fluorescent and upconverting inks
    iv. Customized void effects in tamper evident labels, leading to a distinct opening colour change
    v. Tamper evident covering of the unique identifier
b. Covert or semi-covert safety features
    i. special inks, taggants, markers, many of them "machine readable" are available in various levels of security (=out of the reach of counterfeiters) and pricing

We share the opinion of most parties involved in the discussions, that the choice of safety features, which shall be applied in addition to the unique identifiers, shall be left open to manufacturers, to allow for technical development, competition among suppliers, and making it harder for counterfeiters.

Such "authentication technology" is available at various price levels from very low to very high, i.e. from 0,01 cent per package to 10 cent per package. On an average however, the unique identifiers - to create them, print them and run a verification system - cost more than many other safety resp. authentication features.[2]

The Directive mentions cost considerations, which are of course important, given the financial situation of some of the European health insurance systems as well as players in the pharmaceutical industry.

Whereas the Directive does not foresee a differentiation of requirements among prescriptive drugs with regards to level of authentication features and tamper evident features, we believe that a differentiation will be necessary, based on a risk assessment of the specific drug.

Medicines of high impact / market price / attractiveness for counterfeiters[3] will have to bear safety features in addition to the Unique Identifier. More important, medicines of higher risk will also have to carry reliable tamper evident features. Only in combination of all three

[2] This cost statement is based on Securikett's own calculation of the Codikett® UID system we offer, as compared to other safety features we offer.

[3] It has been found, that not only do expensive products get counterfeited, quite often the quantity of items sold is what makes a product more prone to be counterfeited, even if the item price is low.

- identification
- additional authentication features
- reliable tamper evident features

it can be guaranteed to a very high degree, that the content of such a medicinal package is original.

For other medicines which are less at risk, be they prescriptive or OTC, the unique identifier in combination with a simpler tamper evident feature may be sufficient.

Thoughts about Exceptions from a Security Point of View

The Directive provisions exceptions regarding OTC products and some prescriptive medicines of lower risk to be counterfeited. These products will not need to have safety features, unique identifiers and tamper evidence.

We want to highlight some problems connected:

- Pharmacists, healthcare professionals and patients may be confused,
- Counterfeiters may use this uncertainty to find leaks,
- Counterfeiters will redirect their efforts to products that do not bear any safety features, they will seek their second best choice so to say.

Due to the high cost of the introduction of the Unique Identifier, it is legitimate that many benefits, other than identification and traceability to the manufacturer, shall be achieved by their use. Such benefits may include

- reimbursement,
- supply logistics,
- compliance (not picking the wrong medicine by the pharmacist),
- organizing a recall,
- and further benefits by online connectivity through the Unique Identifiers.

Although we believe there are cost reasons to exclude medicines, due to their lower risk, we recommend encouraging those to bear the unique identifier however, to foster uniformity of use in the market and for the benefits of the identifier which goes beyond anti counterfeiting.

Mr. Domenico Di Giorgio (Director of Counterfeit Prevention Unit of Italian Medicines Agency AIFA) pointed out in his presentation given in Geneva on November 3rd 2011, that since the introduction of the “Bollini” System in Italy they observe that counterfeiters started to declare their “medicines” as non prescriptive alternatives to the real products to circumvent the control established by the “Bollini” System.

Proposing an Open Architecture for Unique Identifier Systems[4]

In discussions around the realization of the Directive's requirements with regards to identification, we often find the following concept:

1) unique identifiers (UIDs) are generated
2) UIDs are assigned to packages of a specific product and batch (printed directly, using labels etc.)
3) UIDs together with their reference data (manufacturer, product type, batch …) are entered into a database, called repositories system
4) As products cross borders, the UIDs are moved from one national database to the database of the new destination
5) When a product is dispensed in the pharmacy, its UID is deleted from the database[5].

There is nothing wrong with this basic concept, which would work well on a smaller and simpler scale.

The goals of this concept are clear. However in modern IT the volume and complexity of the data movements as described above can be solved much more cost effective.

There are two new concepts, which in combination enable a very flexible system, leaving manufacturers independent, their privacy untouched, and which can start practically any time.

One concept is about using attribute data management, the other concept is about interoperability of systems following the new emerging ISO standard.

UID systems are more than repositories

In the directive the term "repositories system" is used, which may be misleading, since it pretends to stand for a database containing the unique identifiers mainly. In this introduction we use the term "UID system" as a term for a system that has at least some basic functions as follows:

1) Accepting a query for verification
2) Processing the query to verify the UID (the UID being an unguessable code)
3) Processing the UID to retrieve the correct reference data or "attributes"
4) Sending back a response resp. data to the inquirer

To make this possible, the system in a first step needs to have services that

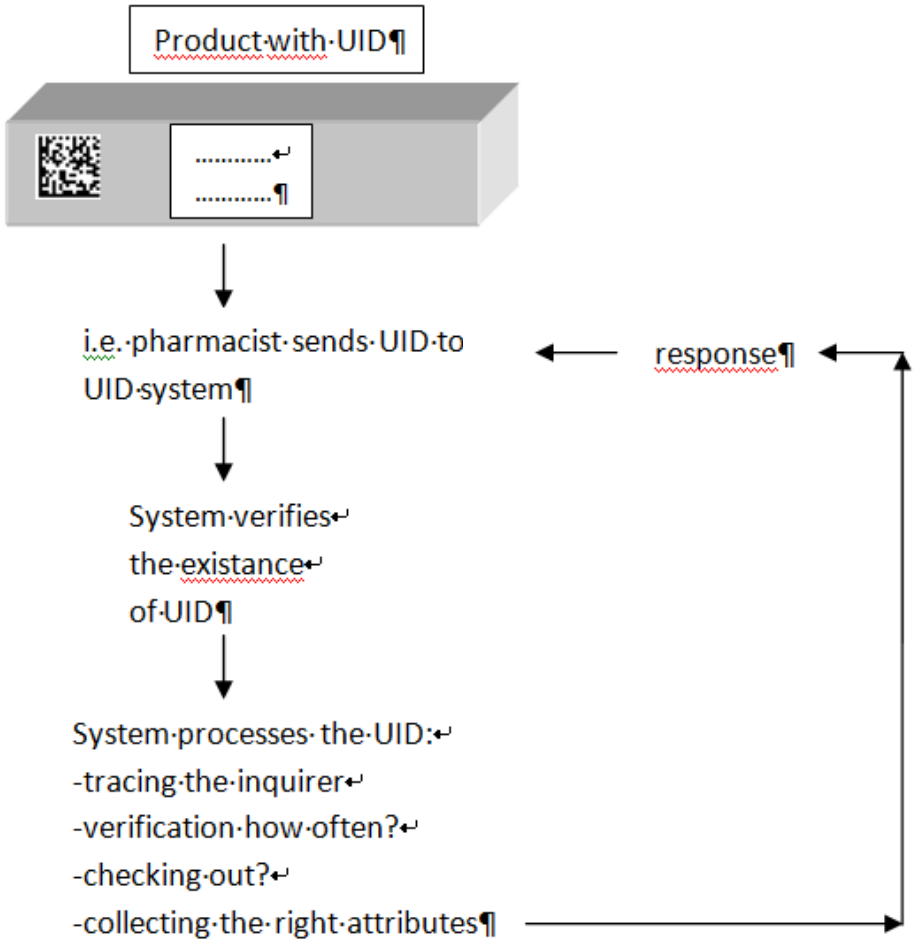
(a) Create UIDs
(b) Provide them for assignment to products
(c) receive "attributes" such as information, content, reference data that shall be linked to the UIDs reps. the products they mark

[4] For simplicity we do not mention in this section, that the per item UID will most likely be printed in combination with a per product group GTIN, expiry date and lot number, in a GS1 Datamatrix format, since this does not affect the basic questions.
[5] Traceability shall be immediately deleted?!

Such systems can be run by various parties, such as pharmaceutical companies themselves, IT and security service providers, governmental entities etc. It can also happen that not all functional units as described above belong to the same entity.

We assume there will be many independent UID systems, as there are already now some systems of this type in the market.

In order to be acknowledged for use in the field of anti counterfeiting, UID systems have to follow stringent security rules, not only with regards to the creation and handling of unguessable codes, but also with regards to vetting their employees, suppliers and customers. In short it needs security management in order to be a UID service provider.[6]



Basic transactions in a UID system

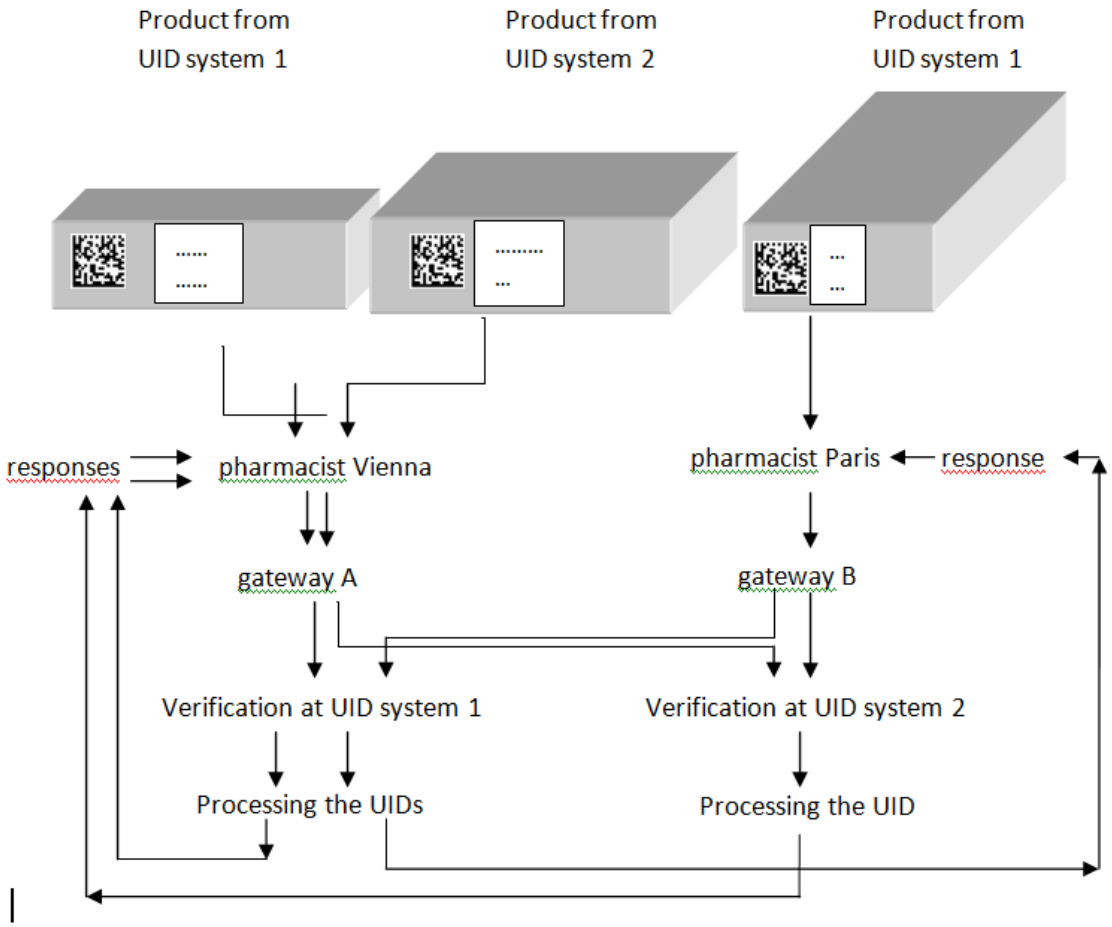
[6] ISO TC247 WG1 is working on "Security Management Systems - Fraud countermeasures and Control", the name of the committee draft is CD16125. ISO27000 on IT security will also have to be considered.

Gateways Make UIDs Systems Interoperable

Between above 1) and 2), thus between sending a query and getting it checked, a gateway is needed, that redirects the queries to the respective providers of services. Thus the UID systems become interoperable.

Gateways would be able to accept UIDs from many systems, redirecting them to the systems they belong to. There may and should be many gateways to accomplish this. They could be run by EU member states themselves, by public agencies etc.[7]

Communication between gateways and UID Systems is preferably handled by means of an encrypted data transfer including a mutual authentication. This can be easily achieved by using a protocol like "AS2" which is standardised, easy to implement and widely used for such purposes. Every participant in the compound system has to have a "passport" in the form a digital certificate which identifies him unambiguously and protects the communication at the same time.



Interoperability by trusted gateways and standardized UID systems

[7] Gateways with a rerouting function to access different UID systems, may also be at the data entry point of such systems, as a good practice.

This basic architecture has some substantial advantages compared to national databases containing all the data:

- Data traffic can be reduced by an order of magnitude because no data has to be moved around. Functions that would be needed to move the data can be completely avoided.
- Stakeholders like customs authorities can be easily integrated in the architecture. Their worldwide system (WCO) simply gets entitled to act as a gateway as well, limiting the information to what they need to know. With national databases in use a customs official checking a potential counterfeit would have to query ALL national databases before he can tell it is a counterfeit (because none of the national databases "knows" the UID).
- The data privacy of manufacturers is protected. They remain in control of their data because the data never leaves their systems or the systems of their service providers. They simply have to react on verification requests in a uniform way.
- Special needs of national bodies (e.g. reimbursement issues) can be implemented on the gateway level keeping the functionality of the verification level untouched.

Attribute Data Management Goes Beyond Simple Data Bases

To pinpoint the benefits of UID systems, let's look at a state of the art attribute data management[8]:

- content attached to a product may be in different languages, the right language will be picked by the gateway
- content sent back to the inquirer depends on his user rights
- content sent back to the inquirer may also depend on the gateway by which the query enters, for example a national gateway will be able to get the right reimbursement number valid in that EU member state
- content such as "destination market" may be easily changed online, without moving all the data from one database to another
- a recall may be entered into the verification system by the rights owner at any time. Because it would be based on the lot number it would be a simple entry in the verification system. If the lot (and with it the UIDs belonging to this lot) were distributed to various national databases, they would have to be detected first in order to be able to change the attribute.

It's all about the UID being just a pointer to a content system on the web, this content in IT language is called attributes. It will be important, to allow for an open architecture of multiple up to date systems and services, to draw on the potential of attribute data management now and in the future.[9]

Benefits of an Open Systems Architecture

Pharmaceutical companies should not be forced to take upon themselves the cost of printing UID codes, without having access to these benefits, for example of attribute data management. This would be the case, if the UIDs would be mainly stored in public databases, and deleted when used.

[8] We draw our expertise on attribute data management from developing and providing such a service, called Codikett®. There are other such systems in the market with similar structures.

[9] One of our customers liked the idea, that by checking the code, the name of a medicine or parts of the leaflet may be read out loud, helping patients with decreased visibility.

It would be up to each company to choose its provider or develop an own system, which best corresponds to our perception of free competition.

Pharmaceutical companies would remain under control of their sensitive data. Public gateways would just link and reroute, and would not necessarily extract data themselves.

As time goes on, better and more efficient systems will evolve for the benefit of all.

IT experts say, that by this type of open architecture, a systems collapse is less likely to occur. This is due to the decentralized structure, but also to the internal structures of modern systems as opposed to central databases.

What is a Format, what is a System – about the Relevance of GS1 "Standards"

Knowing that the group of persons working on the delegated act are experts, we still want to recall, what is causing some confusion in the public debate.

This is due to a mix of concepts about what is a printing format, a data structure, and a system for identification of single items. Further confusion is deriving from the concept of standards and what exactly is being standardized, a format, a structure or a system ….

Printing Format

Any value, number or code such as **AZ76HB** may be displayed as

Human readable: **AZ76HB**

Barcode (several types available):

2D Code (several types available):

Stored electronically on an RFID (radio frequency identification device):

This printing resp. storage format has nothing to do with the content of the code. In the above example they would all have the same content: AZ76HB.

Data Structure

By this we mean the way, how a value is composed.

A unique identifier, for example **AZ76HB**, may be formatted in many ways such as

Just the UID **AZ76HB**

As part of a GS1 data matrix, composed of GTIN/ expiry date/batch number/UID, and this structure may look like this:

(01)09099999543217(17)120521(10)1234567890(21)**AZ76HB**

What Does GS1 "Standard" Mean?

When we talk about a GS1 standard, we mean the convention on

- Print format as ECC200 Datamatrix 2D Code:

- The data structure, whereas in brackets GS1 standard identifiers are used, for example (21) being the identifier for the UID part of the code (01)09099999543217(17)120521(10)1234567890(21)**AZ76HB**

- And about the existence of and access to a global directory on the GTINs, which is better known as "EAN codes".

Unique identifiers (UIDs) may form part of such a larger composed value in the GS1 datamatrix structure. This is very likely to be implemented as a way to fulfil the directive's requirement for identifiers, taking along the benefit of the introduction of GTINs (EANs) for logistics and trade.[10]

Systems as Opposed to Formats and Structures

By GS1 standard we do not however mean a standard on how the system behind should work, which is what we have described as UID systems above. ISO WD16678 is working on the basic definitions on such UID systems and their interoperability.

GS1 as a global, not for profit organization may want to develop and offer such UID systems also, thus enlarging the scope of their manifold activities.

[10] GTIN, batch and expiry date will be part of the online "attributes" of the UIDs also. To be able to read them immediately, without online connection, the direct print as part of the GS1 data matrix makes sense.

However this is not required when it comes to using the GS1 Data matrix format and structure, this structure may be used by any independent UID system provider. As mentioned, pharmaceutical companies themselves may run their own and proprietary UID systems, same as third parties.

How Can GS1 and an Open UID System‘s Architecture Be Linked Together?

Let’s recall: In an open architecture trusted gateways will reroute queries to the respective providers of the UID service providers or systems.

For the gateways to be able to do so, they need to find out, where to reroute the UID to, when a query arrives. This may be done in two ways:

1) There is an application identifier attached to the code, which identifies the UID service itself. For example before the (21)AZ76HB there could be (41)123, whereas (41) is an application identifier for a UID service provider, and 123 is the specific name of the service. The GS1 formatted code of above would change from
    a. (01)09099999543217(17)120521(10)1234567890(21)**AZ76HB**
    b. To (01)09099999543217(17)120521(10)1234567890**(41)123**(21)**AZ76HB**
2) The GTIN directory, run by GS1, would have the information on the relevant UID system provider. For each GTIN (type of product), that uses a UID system, the name of the system would be revealed upon reading the GTIN and accessing the GTIN directory (called ONS). The GTIN directory would thus take the role of a gateway. There are some drawbacks in this solution, such as how to handle one GTIN using several UID systems, which we think can be solved.
3) A variation of the approach as outlined in 2) could be a mapping of the GTIN to the provider according to a list at the gateway to be maintained there. Such a mapping list may be centrally administrated and distributed to the gateways on a regular basis.

In the context of the European Falsified Medicines Directive we believe that all three options would work.

However more independence for specific requirements on member state level may be attained by running independent gateways, reflecting the specific selection of attribute data desired in that member state - see above attribute data management and the ability, to retrieve i.e. a national reimbursement number, content in the right language etc.

For this national independence, options one and two can also be linked together, details to be discussed.

Suggestion for a European Architecture

Having outlined how independent systems may work and interoperate, we see the European architecture resp. the roles assigned as follows:

1) EU level:
    a. setting the rules on the principles of the architecture (i.e. open interoperable systems)
    b. consensus on the minimum features and level of security of participating UID systems
    c. Requirements on timespan of data to be kept. For reasons of traceability we are very sure that (some) data have to be kept longer than issuance of the medicine itself
    d. Establishing a certification authority for a secure communication of all stakeholders involved. Administration of accredited stakeholders.
2) National member state level (government resp. industry associations):
    a. requirements for content to be retrieved upon queries such as
        i. verification of UID
        ii. recalls or warning messages
        iii. reimbursement code(s) per country
        iv. logic rule to hinder double reimbursement
        v. name of product
        vi. national register number of product based on GTIN
        vii. Access log of privileged queries (i.e. wholesaler's or custom's check)
    b. Requirements for data download upon queries
        i. Probably a selection of the available content
        ii. Name/code or the pharmacy doing the check
        iii. privileged inquirers – who, what content shall they receive?

3) Gateway level:
    a. Identifying the UID system provider (only allowing for legitimate or accredited ones)
    b. Possibly sending forth the information, for which national member state the attribute data selection has to be done

4) UID systems level, run by pharmaceutical companies or third parties (Codikett® could be such a third party), doing all the main work and processes as described on page 6:
    a) Accepting a query for verification
    b) Processing the query to verify the UID (the UID being an unguessable code)
        i. Processing the UID to retrieve the correct reference data or "attributes" GTIN of product
        ii. Expiry date of product
        iii. Batch number of product
    c) Sending back a response resp. data to the inquirer (it is to be discussed whether this shall be done directly or via the gateway, considering the sensitivity of data we assume a direct response, not going via the gateway, should be better)

To make this possible, the system in a first step needs to have services that

d) Create UIDs
e) Provide them for assignment to products
f) receive “attributes” such as information, content, reference data that shall be linked to the UIDs reps. the products they mark
g) recognizing repeated verification (i.e. because of code-cloning)

Steps to Realization: Feasibility Study by Running a Pilot

A system as suggested is attainable within short reach, since all the components are there, yet interoperability does not exist in full anywhere. The German car parts industry has come quite close to this model with a running system, which is similar, but simpler and less interoperable.

ISO TC247 WG3 is working hard to elaborate the last details for a guideline. In this committee experience is brought together from the microelectronics and semiconductor industry as well as from the pharmaceutical industry, GS1 is working in it, and several UID systems providers resp. users are active members of the team.

Securikett offers to participate in a pilot to verify the viability of the open architecture. Also KURZ is offering to participate in such a pilot for interoperability. It will take less than a year to finalize the feasibility study.

Some calculations on data to be stored and traffic to be handled.

Assumption based on figures published by vfa [11]:
In the EU 10 billion packages of medicals are sold per year.

This leads to a rate of 150.000 – 500.000 verifications per minute (tpm)
In a layered and distributed architecture as proposed, this load can be handled by standard hard- and software.

In a centralized system this can be considered a very heavy workload requiring a special infrastructure. To make it worse – because of the central storage of the data needed for the verification the rate of transactions needed to move the data to the central database has to be added. Therefore the load will be even 3-4 times as high, as for the pure verification.

The most demanding architecture would be to have national databases (by some people called repositories). To synchronize these and to exchange data between them would require transaction rates which can be expected to be at least 10 times higher than in a layered architecture as proposed

[11] Statistics 2011 „Die Arzneimittelindustrie in Deutschland”

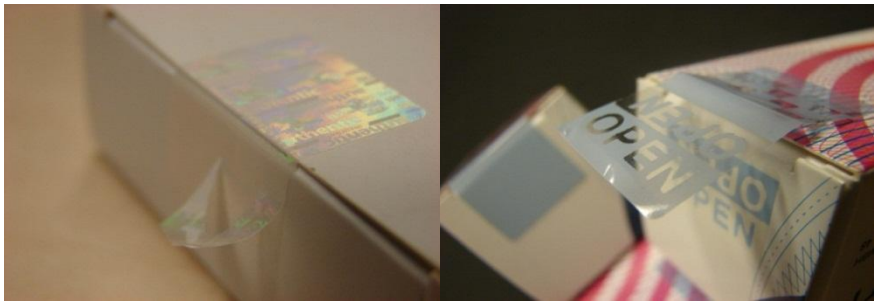
Labels? About Benefits in Using Labels in the Context of the Directive

Labels are parts of packages and may have very many functions and qualities. Being acknowledged as one of the leading developers and suppliers of security labels and in particular tamper evident labels for pharmaceutical boxes, we want to share a few thoughts.

Tamper evident labels

Closure labels or “seals” may be used to follow the requirement of tamper evidence. This is the topic of CENTC261, a European standardization committee set up to outline a meaningful interpretation of the directive with regards to its tamper verification requirement.

We want to mention, that very simple tamper evident labels can be falsified together with the box and everything else. Glued boxes can be easily opened and reglued without notice. For this reason a box of an “exposed” medicine should bear a real security packaging, combining tamper evident closure with security features and the UID code.

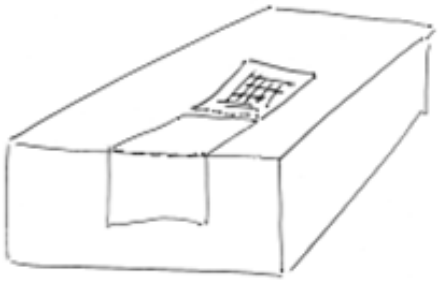


Labels containing the UID

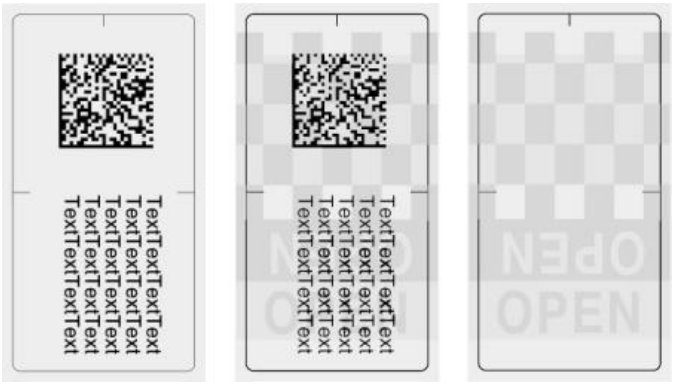
This can be useful in several ways:

1) Using preprinted labels with codes on (i.e. GTIN, UID), such that a pharmaceutical manufacturer does not have to print the codes himself. Talking to smaller firms it seems this will be their solution of choice, whereas larger entities rather tend to develop the organizational structures and equipment necessary in order to print on site, onto boxes or unprinted labels.

2) If a package is very small, the GS1 format together with the human readable parts may not fit onto it. It is offered to print such labels with a “lift-off” part, which can be lifted and the text on the package underneath remains readable. These labels could receive their codes at the label manufacturer or at the pharmaceutical company.



3) There may be other reasons, why it will be cheaper or better to print the code onto a label and then glue it to the box, than printing directly onto the box. Often, tamper evidence and a code are combined into one label.



Questions Set in the Consultation

Some of the following refers to the concepts presented above.

Consultation item n°1

In order to make sure that at the point of verification only one reading device will be needed to verify UIDs from various manufacturers it needs a harmonization of the representation (printing format) of the UIDs. In that sense option 2 is the only sensible choice.

On the other hand the construction of the content be left to the industry as long as it complies with the standard set forth in a liberal way. For the UIDs it should be sufficient to limit the representation to a maximum number of alphanumeric characters.

Consultation item n°2

The industry itself seems to want to go for the GTIN, which is however something voluntary. The advantage seems to be that two improvements can be attained in one,

- one being the logistics improvement by using the GTIN (=manufacturer product code),
- and the other to be seen in raised security against counterfeiting by use of an (unguessable) unique identifier.

However having a closer look, these two may be reached rather independently, by printing the GTIN together with the box (using a cliché or printing plate, not extra cost), and printing the unique identifier in a digital printing mode, be it directly onto the box or by using a label that contains the UID.

Labels with UIDs only, not containing the GTIN, tend to cost less, since they can be manufactured in high volumes ahead of time.

Consultation item n°3

To add batch number and expiry date to the UID is not a bad idea for practical reasons, in particular if it is displayed in a human readable form (like 10/12/2015) also.

However it is not necessary: As soon as the unique identifier is verified, which will have to be done online anyway, the batch number and expiry date can be downloaded as well.

The only disadvantage of printing additional information together with the UID, is again: labels or boxes supplied with the UID already on cannot be used in many cases, because batch number etc. is known only shortly before production in many companies. For this reason pharmaceutical companies will have to invest quite some money into online 2D code printing equipment and vision control systems for all their packaging lines.

The cost of labels – i.e. tamper evident closure labels – containing the UIDs already printed – would be lower, as compared to print them at the pharmaceutical manufacturer, because overall less digital printing equipment will be needed.

We see cases, where the UIDs (with or without GTIN, expiry date etc.) will have to be printed onto labels anyway ("lift-off label construction"), because some boxes are really small. The printing of codes onto the labels could be done at the pharmaceutical manufacturer or at the label printer.

Consultation item n°4

We are against option 2. The reason for this is, that the code would always have to be replaced if an item crosses the border.

Option 1 is ok. We assume, that per country one GTIN (product code) is related to one reimbursement code only.

By attribute data management we can offer a third solution: the reimbursement code will be returned upon a query of the UID (for verification). Having one unique ID, it may return country specific reimbursement codes, depending by which gateway the query is entering the verification system.

Consultation item n°5

We are in favour of the 2D barcode. Main reason: in order to create a state of the art unique identifier, that does not repeat, cannot be guessed, 16 alphanumeric digits are quite commonly accepted by experts in mathematics or cryptology. 16 digits are almost impossible to print as a barcode onto a small pharmaceutical box, because it gets too long.

We estimate a 2Dcode reader to be connected to a computer to cost less than 100 Euros, maybe just half of this. Smart phones are able to read 2D codes also.

RFID is not resistant against manipulation – the chip may be smashed – so an additional print is advisable, then again as a 2D code. RFID may be interesting as an additional device, in cases where cost is not a main concern.

Consultation item n°6

There are other interested parties who do random checks of unique identifiers, already today, these are

- customs authorities
- intelligence agents of the brand owner (often third parties)

And

- possibly governmental agents will randomly check whether the Directive is followed.

At this point we want to recall the concept of "user groups", these are interested parties to send a query, disposing of different authorizations, which they send along like an electronic certificate, using i.e. a password.

In order to "check out" an item of a system, as opposed to just "checking along the supply chain", these users have to identify themselves at different a different level in a user hierarchy. Any party, now or in the future, which is eligible to dispense pharmaceutical products, can be given the rights of

this user group. They'll have to identify themselves in an appropriate manner with regards to IT security.

Modern systems use the concept of a verification count, rather than deleting a code from the system. The system would know, which queries have been done by which parties, and who and when has "checked out" the item. The item code will remain alive for some more time, warning the next one to check the item out (verification count i.e.: "Warning: the item is already checked out and you are the third one to try this again").

The reason why we think the UID should not be deleted immediately: We would delete evidence in case of counterfeits such as cloned codes. European and or national legislation should set a rule, how long after end of expiry date a code should not be completely deleted. We have in our minds this could be three more years, but it's up to pharmaceutical experts to decide this. If the expriy date is also printed as human readable directly on the package, as is expected, we think two or three years should be enough.

Consultation item n°7

We think random checking is the best to do, and there should be rules about this (i.e. 2 per palet, 1 per transport box upon smaller shipments …), whereas only the pharmacist should verify and "check out" every single item.

Random checking is not connected to a lot of cost, other than the time to do it, since a computer and internet access are standard in every office now, only a 2D code reader may have to be purchased in addition. For simple checks without dispensing, smartphones may be considered also.

The main cost issue will be the time used for opening the transportation box, and doing checks. For this reason, random checks will be more cost efficient than complete checks. Wholesalers could be audited from time to time to show their evidence on this checking.

By establishing a user hierarchy, there will be no problem with checking out single items too early.

There is a security rational against too much checking along the supply chain, and in particular against scanning all the UIDs! Fraudsters working at the wholesalers could then easily forward all the UIDs they have scanned to counterfeiters, who might then try to bring their product to the market faster. So we suggest not to allow scanning all(!) the UIDs.

Consultation item n°8

We support option one, called "stakeholder governance". This enables lean UID systems to be employed. Within the context of the Directive, UID systems are called repositories systems. Leaving the development and cost of interoperable systems, as outlined in our introductory chapters, to competition, guarantees for the best cost structure. Also gateways to make interoperability work may be run by private parties.

We can see a possible hybrid solution between option one and three. So nation states or national industry associations could also offer UID systems, to enable smaller players to participate. However the same may be achieved by third parties offering such systems.

By stakeholder governance, repositories systems – we call them UID systems - can start their activities any time. A gradual (!) start of the work is possible. By experience with one of our customers, it took them several years to roll out serialization globally and the process is not yet finished. So a gradual start may be usefull by allowing for a longer changeover time, and this may start rather soon.

It is important that certain rules are set by the European / national legislation – see above "suggestion for a European Architecture". For example there will be minimum attributes (attached information) for each item to be sent back by the system upon a query. It has to be unified, what minimum data shall be downloaded to the pharmacist (if any).

Consultation item n°9

In a context of anti counterfeiting it is important for manufacturers to know where and by which routes their products reach the market.

We fully acknowledge the fact, that manufacturers or pharmacists should not be able to collect the identities of users/patients due to privacy.

It is not understandable why manufacturers should now (finally!) resume their responsibility to act against counterfeiting, bear the cost to run such systems, but then should not be able to track their products. We do not say this as pharmaceutical manufacturers (which we are not), but by being part of the anti counterfeiting community. In a global context it becomes evident, why distribution data should be made accessible to manufacturers (and other more neutral parties?). When counterfeits enter the scene, illegal diversion often plays an important role, in the global perspective.

To resolve the dilemma of privacy versus traceability rules have to be set by legislation. UID systems will have to be audited in this respect, not matter if they will be private, national or European.

One advantage of private systems ("stakeholder governance") is that at best a manufacturer can see his own distribution channel data, but never those of his competitors, nor any other data of a competitor.

Consultation item n°10

Ad 4.2. It will be important, that if reimbursement will/can be conducted simultaneously with the checking of UID / checking out the UID at the point of dispense, the reimbursement number and patient insurance number will be sent away (!) to another system, probably run by the insurance authority. This procedure should not be within the UID system (called repositories system in the directive). The UID system should just forward the reimbursement code to another system. This way it can be guaranteed, that no patient identification is put back into the UID system.

Ad 4.3. Talking about equivalent safety features is always problematic, because several manufacturers are already now employing further open and hidden features to protect their product against counterfeiting. As stated in our introduction chapters, products at risk should have those safety features in their original meaning (taggants, holograms, security inks, customized void-effect etc.) in addition to the unique identifier.

Some are called forensic features (for proof in court), because they are not visible, thus the re-packager cannot even know that he should replace them.

We suggest, that together with registration it should be published to the national authorities what other safety features a package bears: not which one in detail, because that would erode the security, but which types. That could be for example:

- hidden substance
- visible substance
- visible special ink
- holographic features
- colour change upon opening (void effect)
- printed features (moire, microtext, guiloches)
- private representation of unique code
- others

The re-packager would then have to replace by a feature of the same group, and keep some specimen of the original packages he has replaced for later traceability (did he repackage a fake or an original?)

With regards to the UID, we suggest:

Booking out the UID, replacing it by a new one, and creating a UID by UID replacement datafile for traceability. This would be just like a quality document, not to be posted anywhere.

To reuse the UID already on, i.e. reprinting it piece by piece, is too close to acts of counterfeiting, we would not suggest this.

Overall we believe that legal repackaging, as is allowed in Europe, should be a distinct, well visible, well traceable act. The re-packager, being a “manufacturer” now in the eyes of legislation, will have to write his name and identity on the new pack he is creating, maybe as part of an additional label. That label could then cover other functions such as tamper evidence, or even carrying the new UID.

Consultation item n°11

As stated in the introduction part under “Thoughts about Exceptions ...” we have to first of all consider what will possibly cause confusion for the pharmacist. Any too complicated black and white list scheme will be confusing and possibly open doors to counterfeiters.

In China I could observe that all OTC products have a well visible “OTC” logo on their packs, leading to a clear distinction for everyone. Such a logo could eventually be introduced in Europe also, plus one for “prescriptive” and one for “prescriptive, but no safety features”.

We think that the latter concept of “prescriptive, but no safety features” is not advisable, since it seems likely that reimbursement will be taken along, which would then require them to bear the UID anyway.

As discussed in the introduction part we are in favour of:

Prescriptive medicines at risk (high overall revenue, high impact on patients) should bear at least

- Unique identifier
- Reliable tamper evidence (more than a glued box)
- At least one safety feature in its original meaning

Prescriptive medicines at low risk should bear at least

- Unique identifier
- Tamper evidence (simple solution acceptable)

It has to be considered that by excluding some prescriptive medicines, this will make them more attractive for counterfeiters, being the only “holes in the fence”.

Reading through this part of the consultation we want to remind of the fact, that several manufacturers already use UIDs, use tamper evidence or use safety features. This is not only done for medicines, but also for healthcare products (surgery equipment!), or animal healthcare or agricultural medicines, all of which may be affecting human health again.

It must be left with the manufacturer’s choice and sense of responsibility, to implement such features whenever they find it appropriate. The Directive may require certain minimums in protection, but should by no means inhibit other medicines or products from being protected!

Consultation item n°12

Criteria 2 are problematic in the case of new medicines. Else the scheme looks good. It is not within our competence to judge about the weight of criteria. As stated above, we are in favour of a graduation of the amount of security and think it will not be useful exclude any prescriptive medicines from the Directive in the long run. This would erode

- Security against counterfeits
- Logistics improvement
- Less dispensing mistakes
- Less medicines sold when expired
- Reimbursement conducted in a more automated way
- Etc.

Many of these benefits have been established by the industry associations, not by the Directive. For these reasons and benefits the use of UIDs seems to become the (!) safety feature solution, before others, and this seems to be what pharmaceutical manufacturers are ready to invest in. These benefits would be deluted or even not come to life, if exceptions are made.

List of References

Richtlinie 2011/62/EU des Europäischen Parlaments und des Rates vom 8. Juni 2011 zur Änderung der Richtlinie 2001/83/EG zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel hinsichtlich der Verhinderung des Eindringens von gefälschten Arzneimitteln in die legale Lieferkette, Text von Bedeutung für den EWR, siehe

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:174:0074:01:DE:HTML, accessed October 24th, 2011

EUROPEAN COMMISSION,HEALTH AND CONSUMERS DIRECTORATE-GENERAL, Health systems and products Pharmaceuticals, Brussels, 18/11/2011, Sanco.ddg1.d.3(2011)1342823, **DELEGATED ACT ON THE DETAILED RULES FOR A UNIQUE IDENTIFIER FOR MEDICINAL PRODUCTS FOR HUMAN USE, AND ITS VERIFICATION, CONCEPT PAPER SUBMITTED FOR PUBLIC CONSULTATION**

http://ec.europa.eu/health/files/counterf_par_trade/safety_2011-11.pdf , accessed April 13th, 2012

COOPERATIVE INTER-SECTORIAL STRATEGIES TO COUNTERACT COUNTERFEIT MEDICINES: THE ITALIAN EXPERIENCE, Domenico Di Giorgio, Director of Counterfeit Prevention Unit of the Agenzia Italiana del Farmaco (AIFA), Presentation given in Geneva on Nov. 3rd 2011

ISO 12931:2011 "Performance criteria for authentication solutions for anti-counterfeiting in the field of material goods"

ISO/WD 16678 „Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade“

ISO PWI 16125 „Security Management System - Fraud countermeasures and controls“

ISO CD 14298 „Management of security printing processes"

CEN TC261 /SC5/WG12 “tamper verification features for medicinal product packaging”