

TAX STAMP SPECIAL REPORT

ISSUE 1 / 2016

ANATOMY OF THE MODERN TAX STAMP



PUBLISHED BY

RECONNAISSANCE
TAX STAMP
NEWS™

Welcome

What does an excise tax stamp look like today, compared to what it used to look like? What are the drivers that have shaped the modern stamp and what are the individual parts of that stamp that make up the whole? What role does the stamp have today that it did not have before?

These are the questions addressed in this first special report, devoted to the anatomy of the modern tax stamp.

The report dissects the stamp and describes the characteristics and function of each dissected piece – from the material elements of substrate, printing methods, ink and multilevel security features, to the digital elements of unique coding and associated track and trace systems. The report also looks at the tax stamp as a whole by referring to different stamp programmes currently being used across the world.

Fifty years ago, tax stamps were nothing more than simple pieces of paper, with little or no security and no serialisation, serving as tax collection tools and proof that the correct tax had been paid on the product they were affixed to.

Today, as a result of various fiscal and socio-economic developments, combined with technological innovations in security printing, serialised coding, data processing and mobile communications, tax stamps are transforming into sophisticated devices with additional roles that relate to product authentication and supply chain security.

Each element of these ‘sophisticated devices’ will be covered in detail in this special report.

We would like to thank all the organisations that have supported the report as sponsors, as well as all those that have contributed to its content. We could not have produced it without their help and are delighted that they have recognised the value of such a publication.

We trust that the report will provide a useful tool for all readers to become more familiar with both the material and digital components of today’s tax stamps, as well as their accompanying track and trace systems.

Any feedback you would like to give us will be gratefully received. We look forward to hearing from you at

publications@reconnaissance-intl.com.

Nicola Sudan
Editor, *Tax Stamp News*

Editor

Nicola Sudan of Reconnaissance International, is editor of the *Tax Stamp News*™ monthly newsletter, and director of the annual *Tax Stamp Forum*™, attended by 250 delegates from stamp issuing authorities, enforcement agencies and supplier companies. She has more recently been appointed General Secretary of the newly formed International Tax Stamp Association, founded by ten leading tax stamp and component producers to promote the highest professional standards within the sector.



Taggants: the Final Frontier

This chapter looks at the microscopic or molecular particles known as taggants and their use as covert and forensic markers in tax stamps.



Taggants are a staple of the document and product protection industry. They have achieved rapid growth in recent years, in large part due to their anonymity, versatility and flexibility. In fact, the number of companies supplying taggants has about doubled over the last ten years.

There are many different types of taggants and while most have a similar purpose – namely the ability through a unique code to provide covert identification and sometimes quantification for identification of product dilution – the underlying technologies have been developed from a broad spectrum of different sciences.

Taggants can be inorganic or organic in composition and exhibit specific and unique physical, biological, chemical or spectroscopic properties, which are typically read and authenticated using a variety of different methods, ranging from a simple microscope, to hand-held detectors to matching assay kits. Most taggants are able to be detected in the field, but some require lab analysis.

In their simplest form, taggants provide a simple yes/no authentication by their presence, or absence, detected by a hand-held reader. The underlying technologies can also provide innumerable variants within the individual taggant particles themselves, allowing different batches of taggants to be assigned different meanings – such as specific departments within an organisation, or production runs – which transforms them into virtual fingerprints or unique signatures.

Some taggants offer almost infinite permutations of codes, while the technology has widened to the extent that a taggant can be engineered to suit almost any product, and if not the product itself, then some part of its packaging.

Taggants are in widespread use in tax stamps. Just as holograms are the principal overt security features for stamps, so taggants have become the most generally accepted technique for covert and forensic identification and authentication.

According to the Forensic Science Laboratory (FSL) of the US Bureau of Alcohol, Tobacco, Firearms & Explosives (which is often called upon to examine potential cases of counterfeit tax stamps), if counterfeiters can see a feature, they will attempt to copy it. Therefore products with covert features, such as taggants, are the most difficult to effectively counterfeit and therefore the easiest to examine.

Having said this, taggant readers for use in the field should be as robust as possible, advises the FSL.

In some cases, taggants may be the only security feature present in a tax mark. The UK, for example, uses a fiscal mark instead of a stamp for tobacco products, consisting of the words 'UK DUTY PAID' written in black on a white background. As the taggant is the only security feature in the fiscal mark, the mark can only be authenticated with a taggant reader.

Taggants are applied to the stamps in a number of ways, embedded in either the paper pulp or fibres, the ink, the holograms or even the adhesives – but they are generally incorporated into the ink.

So what are the different kinds of taggant technologies used today, and which ones are best suited to tax stamps?

Just as holograms are the main overt feature for tax stamps, so taggants are the most generally accepted technique for covert and forensic authentication.

The original taggant

The origin of taggants, and their name, lie with Microtrace's *Microtaggant® Identification Particles*, which is based on technology developed in the 1970s by 3M. The technology consists of an engineered microstructure of different-coloured plastic layers that form a unique numeric code. Microtaggants were initially developed to be added to explosives for identification and tracing purposes, once the explosives had detonated – so it goes without saying that they are very robust.

Microtrace's Microtaggant particles are microscopic – ranging in size from 20 microns to 1,200 microns (1.2mm).

In basic form, Microtaggants are a unique code sequence represented by the different layers of the taggant particles. In more complex forms, Microtaggants deliver multiple layers of security through the incorporation of various materials – such as IR, fluorescent and magnetic properties – within each particle.

Microtaggants are mainly used for product authentication, product diversion tracing and bulk material identification, and can be incorporated into most materials, including security inks (UV flexographic or rotary screen), adhesives or directly into substrates such as plastics and papers.

While Microtaggants can be easily incorporated into adhesives, films and papers for tax stamps, due to the relatively large particle size, it is not possible to print them via the offset and inkjet print methods normally used.



Microtrace LLC's multi-layered Microtaggant Identification Particles.

Microtrace's spectral solution

In response to this printing challenge, Microtrace has created a taggant technology called *Spectral Taggant™* security ink, specifically designed for print applications on items such as banknotes, consumer packaging and tax stamps.

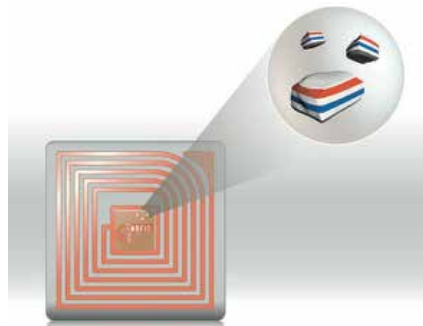


Microtrace LLC's Spectral Taggant system.

Spectral Taggant is a proprietary, multi-component chemistry requiring a proprietary *Spectral Reader* – a sophisticated hand-held device which gathers hundreds of data points per reading to ensure an exact match to the Spectral Taggant signature. According to Microtrace, even a small change in the substrate or printing technique could lead to a failed reading.

3S's microscopic taggants

Another producer of microscopic taggants is 3S Simons Security Systems, with its *SECUTAG®* technology. According to 3S, the SECUTAG micro colour-code particles are the smallest in the world (the smallest particle is 8 microns in size). The SECUTAG taggant resembles a sandwich composed of between four and ten colour layers to form an individual customer code.



SECUDATA combines traceability and counterfeit protection.

The layers are prepared with normal, UV or IR colours and can optionally be provided with magnetic properties.

In its purest form SECUTAG has the consistency of a very fine powder and the codes are printed via all standard printing processes. The particles are invisible to the naked eye; however, a standard pen microscope suffices to identify the code.

The company also offers its *SECUDATA®* solution, which combines different codes and RFID labels for traceability purposes with the counterfeit protection of its micro colour-codes.

According to 3S, SECUTAG's colour-code system has been forgery-proof for over 15 years and is therefore accepted as evidence by courts.

Up-converting phosphors

Up-converting phosphors are microscopic ceramic powders that convert invisible infrared light wavelengths to visible coloured light. Essentially, these taggants light up when hit with an infrared light.

Since up-converting phosphors are a well understood class of materials with many published papers and manufacturers around the world, they are considered to be relatively easy to replicate or mimic, therefore not always recommended as a stand-alone security solution. However, in combination with other taggant technologies, such as Microtrace's Microtaggant, they can be utilised as a step in a multi-level security solution.

In addition, exclusive up-converting phosphors, with specific spectral responses can be developed if required.

Another provider of up-converting technology is the specialist security ink supplier, Luminescence. Luminescence manufactures machine-readable up-converters and down-converters (such as the *Affirm* system). In addition, its machine-readable K2 system consists of inks with a unique light signature, based on fibre optic technology and complex algorithms, which are used on banknotes, passports, tax stamps and ID cards in several countries.



A single Microtaggant Identification Particle with upconverting phosphors, illuminated by an infrared laser pen.

Rare-earth taggants

The most generally used type of inorganic (ie. non-carbon-based) taggants are those that contain elements from a group in the periodic table known as the lanthanides or rare-earth metals. Each lanthanide has unique spectral properties, in the form of narrow band emissions that last for a relatively long time after excitation.

By using different combinations and concentrations, unique spectra are obtained which may be easily and quickly detected using specialised equipment. The lanthanide mixtures are generally embedded in carrier materials that in themselves can influence the code of this mixture, adding to their security.

Unique Identifying Codes

So far, in this report, we have covered substrates, printing processes, holograms, security inks and taggants. All of these components constitute the fixed elements of the stamp, and essentially remain unchanged for all stamps within a particular product category and jurisdiction. Other fixed components include printed markings that indicate, for example, the name of the tax authority.



In this chapter, we turn our attention to the variable components of the tax stamp, which often consist of an inkjet- or laser-printed visible serial number and product description (eg. '20s cigarettes'). In addition, many tax stamps today carry a barcode containing the serial number, product description, and eventually other tax-related data, in machine-readable form. The barcode can also provide an automatic link to additional product, manufacturing and distribution information associated with a particular serial number.

Together, these variable elements constitute an identification code that is unique to each individual tax stamp. This unique code (or UID) provides visibility on the movement of the stamp (and therefore the product it is applied to) and allows it to be traced back to its place of application.

A wide range of different technologies are available today to generate and assign UIDs to tax stamps. These include simple printed alphanumeric sequences, right up to complex codes with built-in security features, based on unique and proprietary technologies that are difficult to generate, detect or manipulate by anyone other than those authorised to do so.

The UIDs are typically recorded in a central database and can be supplemented by information added in the field as the products make their way through the supply chain.

Theoretically, when the system works as intended, a digital picture of the product's progression through the manufacturing process and into the marketplace – called a 'pedigree' – will be available at any time the code is interrogated.

As can be imagined, the process of developing, deploying, managing and utilising the information generated by what can be billions of individual codes can be a huge and expensive challenge. But the promise of these systems is that when properly implemented, they can deliver highly useful patterns of information as to the path of legally produced items in the marketplace and serve as early warning signs of fraudulent activity.

In addition – and something which is vital for those countries experiencing high levels of tax evasion by local manufacturers – the UIDs, together with their accompanying scanning and activation systems, give revenue authorities the ability to automatically monitor local production runs in real time, thereby preventing manufacturers from making false tax declarations.

How are UIDs generated and secured?

UIDs usually consist of proprietary codes generated at secure premises by the tax stamp provider. Alternatively, the codes can be applied directly to the product packaging – which is the case for the *Codentify*[®] serialised marking solution for cigarette packs, where the provider is the tobacco industry itself.



Codentify system directly printed on cigarette pack. Consists of 12-character alphanumeric string, with corresponding DotCode 2D barcode for machine-readability, and two lines of text.

UIDs, in themselves, are not secure and need to be reinforced with safeguards that prevent fraudsters from creating false codes that could potentially pass as genuine.

Such measures begin with restricting access to the code-generation system to authorised personnel only. Furthermore, it is vital to ensure that the code sequence is not predictable.

Other safeguards include a check digit system (where the last digit in the serial number is a check digit generated from an algorithm), as well as encryption, where a string of data elements within the UID is processed using an encryption algorithm. The encrypted string bears no resemblance to the unencrypted string, and the original data elements can only be deciphered with a decryption key.

Another safeguard to detect the presence of an illegally created code is to repeat the code elsewhere on the tax stamp (or directly on the product), such as in the machine-readable barcode.

If the visible code does not match its barcoded counterpart, then the inspector will know the code is false.

Different code formats

A practical challenge to implementing serialisation on tax stamps relates to how the UIDs are printed and read on what can be a very small area. Tax stamps share this problem with pharmaceutical labels, which is another product area where serialisation and pedigree are used.

Although visible alphanumeric sequences can be read with the naked eye, they are difficult to use in the field, since they require the user to input what is sometimes a long and complex string of numbers and letters (some codes are as long as 24 characters).



Example of a very long code produced by Yottamark for its Harvest Mark traceability system on fruit and vegetable packaging. This 24-digit string and accompanying datamatrix barcode potentially enable more information to be associated with the product than a shorter code.

A complementary, machine-readable code format which is gaining popularity in this area is the two-dimensional barcode. The 2D barcode can carry a large quantity of information in a small space, and also contains a built-in error correction mechanism, which allows data to be read even when part of the barcode is damaged or destroyed.

There are a number of different 2D barcode symbologies available today that are used for a variety of applications (a symbology is a protocol for arranging the bars and spaces of a particular barcode, for the encoding of numbers, letters and binary numbers).

The most popular 2D barcodes currently used for tax stamps are matrix codes – in particular datamatrix and QR codes.

Matrix codes consist of black and white ‘cells’ or modules, arranged in either a square or rectangular pattern. Unlike the older, one-dimensional linear barcodes that were designed to be mechanically scanned by a narrow beam of light, matrix codes are detected by a two-dimensional digital image sensor.

Datamatrix barcodes

Datamatrix is a 2D barcode symbology with a very high data density, mainly used in Europe and the US (in fact, datamatrix codes have now been specified by the EU Falsified Medicines Directive as the unique identifier for pharmaceutical products sold in the EU).

A single datamatrix symbol can theoretically hold up to 3,116 digits, 2,335 alphanumeric characters, or 1,556 bytes, although the capacity is influenced by available printing space and the printer resolution. With a capacity like this, however, it is clear that one datamatrix symbol can hold a lot more than just a serial number.

Every datamatrix code is composed of two solid adjacent borders arranged in an ‘L’ shape (called the ‘finder pattern’) and two other borders consisting of alternating dark and light cells (called the ‘timing pattern’). Within these borders are rows and columns of cells of encoded information. The finder pattern is used to locate and orient the symbol while the timing pattern provides a count of the number of rows and columns. The greater the amount of data encoded in the symbol, the larger the number of cells.

Datamatrix is an open standard 2D symbology within the public domain. This means it can be used freely with no payment of royalties.



The new consumer-oriented Ecuador tax stamp for imported spirits carries a secure QR code that can be scanned by the public via a smartphone app.

QR barcodes

The QR code is another type of open standard matrix code, which was originally invented in Japan, and which, like the datamatrix code, has a very high data density. In addition, the QR code has the ability to be decoded at high speeds, hence the name ‘QR’, which stands for ‘Quick Response’.

A single QR code symbol can hold up to 7,089 numeric characters, 4,296 alphanumeric characters and 2,953 bytes – which is about double the capacity of its datamatrix counterpart.

A QR code is characterised by three distinctive squares located in three corners of the code. These are position markers, which allow the code reader to identify the correct way to read the image. A smaller square near the fourth corner is used for alignment: it detects any distortion to the code and allows the reader to make corrections as needed.

In many applications, the QR code is fast becoming the most prominent barcode technology, especially with regard to mobile phone scanning applications. The code can store anything from telephone numbers, addresses, URLs, and even enable mobile phones to execute various commands.

PDF417 barcodes

Another type of 2D barcode occasionally used for tax stamps is the PDF417 (or ‘Portable Data File’) barcode, which is more predominantly present in ID cards and transport applications (such as flight boarding passes). These applications often require huge amounts of data – in the form of photos, fingerprints, signatures, text, numbers and graphics – to be stored within the code itself, without the need to access a database.

PDF417 codes are described as ‘stacked’ rather than matrix, due to the shape of their linear columns, which are arranged in a long, slender rectangle – a structure that calls for high-resolution printing and screen display. This may require investment in expensive scanning equipment, which is often proprietary. Although resolution is also important for matrix codes, it is less so than for PDF417s. Whereas simple mobile applications can easily scan QR codes, PDF417s are more challenging to scan.

In addition to the features that are typical of two-dimensional bar codes, PDF417s are able to link to other barcode symbols, and be scanned in sequence with these other symbols, thereby allowing more data to be stored.

The Physical/ Digital Link

This chapter explores the ways in which serialisation codes can be augmented with material-based security features to link together physical and digital properties.



As we said in the previous chapter, there is a common misconception that authentication and serialisation technologies are interchangeable. In fact, serialisation, in itself, authenticates nothing.

What serialisation cannot tell you is whether a code that has been verified as legitimate by a reader has not in fact been copied from a legitimate product and applied to an illicit one. To address this flaw, digital serialisation needs to be augmented with overt and covert security elements.

As stated in the previous chapter, this becomes especially important in cases of direct marking, where a code may find itself sitting alone on a product without the physical security provided by a tax stamp.

Security inks

One example of such an augmentation is what is currently being used in Brazil as an integrated part of the country's *SCORPIOS* system for controlling and tracking cigarette production. The system consists of an encrypted, standard 2D datamatrix code, printed with security inks that contain specific covert properties. These covert properties are detected by a proprietary authentication device, but are also readable by commercial devices, allowing for aggregation as well as integration with logistics platforms. In addition, the codes for domestic products are printed in invisible inkjet ink and applied on a tax stamp.

Material-based security is especially important in cases where a code sits alone on a product without a tax stamp.

Security inks, used to print unique codes, can offer a wide range of semi-covert, covert and forensic solutions to secure the codes. Apart from the features mentioned above for the *SCORPIOS* system, other examples include magnetic inks and inks with DNA taggants (see Chapter 6).

Fingerprinting

Another group of features that can be used to link physical with digital relates to the intrinsic physical characteristics found in the tax stamp (or product packaging) itself.

These characteristics are known by a number of names, including fingerprinting, and document or product biometrics. But they are all based on the same fundamental premise, which is that the physical characteristics of individual items are unique to that item.

Examples of fingerprinting techniques include the recording of the tiny, naturally occurring singularities in the way that fibres in paper settle. Another detects the unique three-dimensional structure of substrates in a predefined area, while another identifies the chaotic surface pattern itself.

These unique characteristics can be captured, digitised and stored (as a picture or, more usefully – through an algorithm – as a number), providing a way of matching the item with the captured information. As such, the item itself provides the means of authentication, as opposed to other technologies where the authentication feature is applied or added (in the form of taggants, inks and holograms).

Fingerprinting appears to be the option that protects the basic features of the product packaging, and which therefore comes closest to being a true tool to authenticate a trademark.

And because, in many cases, the captured information is converted into serialised item codes that can be stored in a database, there is a logical extension of its use for track and trace purposes.

One example of fingerprinting technology is *Signoptic™* from Arjo Solutions (formerly part of Arjowiggins Security). This patented extraction technology is based on what the company terms the 'biometry of matter'.

The technology works by taking a picture of a pre-defined area of the product or tax stamp – as part of a high-speed industrial scanning process – in order to capture the unique characteristics found in that area. The captured characteristics are then converted into a unique, random digital code, by means of an algorithm. The scanned picture is subsequently discarded, since it has been replaced by the code (or *Signoptic Signature*, as it is called). The code is stored in a secured government database, along with additional production or event data, if required.