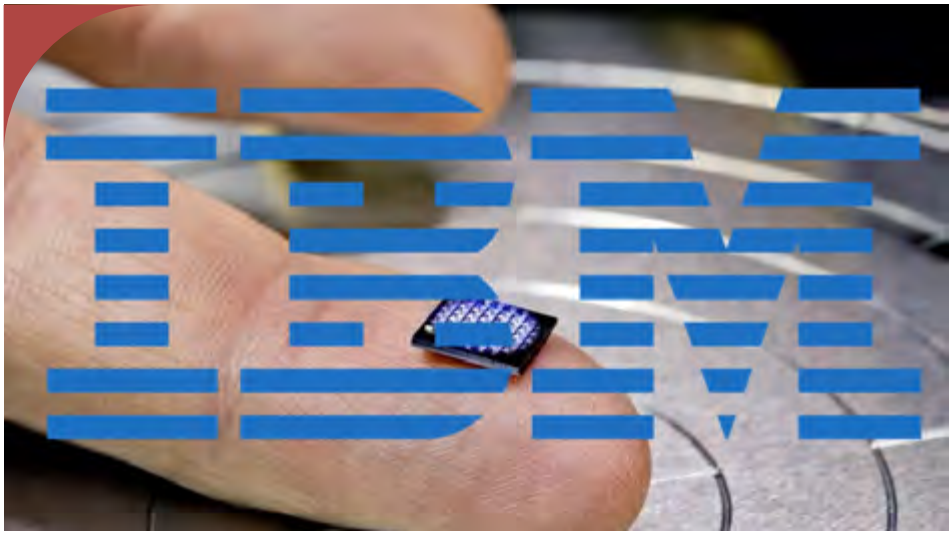
RECONNAISSANCE
AUTHENTICATION NEWS®

VOLUME 24 – NO 4 / APRIL 2018

IBM Predicts Crypto-Anchors will Revolutionise AntiCounterfeiting



IBM Research recently released its annual '5 in 5' predictions (five technologies that IBM believe will fundamentally reshape business and society in the next five years), that showcase some of the biggest breakthroughs coming out of its global labs. One of the five predictions is the use of crypto-anchors, which the company believes will revolutionise anti-counterfeiting.

The crypto-anchors are essentially tamper-proof digital fingerprints embedded into products or parts of products to work alongside blockchain's distributed ledger technology in the physical world.

Several different forms of crypto-anchors have been developed, including a tiny computer smaller than a grain of rock salt, an edible ink which could be stamped on malaria pills and other optical codes that are invisible and have to be activated.

According to the company, the micro-computers consist of several hundred thousand transistors to monitor, analyse and act on data, yet will cost less than 10 cents to manufacture.

IBM scientists have also created a crypto-anchor that combines a mobile sensor (or smartphone) fitted with a special optical device and artificial intelligence algorithms to learn and identify the optical structure and features of certain objects. It can also identify the presence of DNA sequences in minutes.

This dual-enhanced approach (physical and digital combination) to securing the supply chain, according to IBM, is based on the fact that blockchain technology, while identified as the future of transparent digital transactions for supply chains, cannot ensure the authenticity of physical goods by itself.

Continued on page 2 >

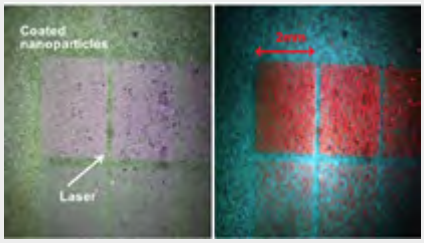
Laser Activation of Nanoparticles

Idvac, the UK-based specialist vacuum metallising developer and consultancy, has developed a new process to activate special nanoparticles using advanced laser technology for covert security applications.

In recent years, nanoparticles have been the subject of much research due to their wide applications in various fields including security. Nanoparticles are tiny particles of materials – that are typically less than 100 nanometres in size.

The light emission properties of nanoparticles are important characteristics for their applications in optical imaging, sensors, etc. However, most of them are characterised by low emission properties.

In this latest development, Idvac has developed a process to specially fabricate nanoparticles. These can be coated onto flexible films such as polyester or paper and then activated by an advanced micro laser technique to exhibit strong photoluminescence properties under the exposure of UV light. By changing the composition of the nanoparticles, strong red or green photoluminescence is observed following the laser activation process.



Coated nanoparticles: Left: under visible light. Right: after laser activation and under UV light.

Continued on page 7 >

Inside this Issue

De La Rue Opens New Product Authentication Facility in Malta

De La Rue Malta facility (© De La Rue).

De La Rue, the world's largest designer and commercial printer of banknotes and passports, recently announced the opening of its product authentication facility in Malta by the Prime Minister of Malta – Joseph Muscat

This announcement follows the opening of the De La Rue Malta Centre of Excellence in April last year (see AN April 2017).

The new facility will produce tax stamps, authentication and brand protection products, including labels for Microsoft, one of the world's most famous brands.

De La Rue's Malta factory, which employs 567 staff, is a centre of excellence across all three of its portfolio areas – Currency, Identity and Brand Protection. The new facility marks the completion of the €27 million investment that started two years ago.

The Prime Minister of Malta was joined at the opening by the Minister for the Economy, Investment and Small Business, Chris Cardona, De La Rue International's Chief Operating Officer Bryan Gray and De La Rue Malta Director Edward Chetcuti.

Prime Minister Joseph Muscat said: 'the fact that a global leading brand in its field has time and time again chosen Malta as a principal base to support its global operations is a certificate of the excellence of our workforce and the honesty of our partnership with industry.'

Bryan Gray, De La Rue's Chief Operating officer added: 'I am very grateful for the long-term partnerships here in Malta which have supported us over the last 40 years. I would also like to extend my thanks to all of the team who are continually recognised for their excellence, across the whole organisation. Malta is a central part of De La Rue's international strategy and we are committed to investing in the future.'

According to De La Rue Malta Director, Edward Chetcuti: 'today gives me real pride because it is another important milestone in our journey in Malta that stretches back more than 40 years and the teams working here are the very best in the world at what they do. Whilst I am deeply proud of them, our heritage and our history, it is the next 40 years that excites me most as we seek to continue to invest and grow our Malta operation as a Centre of Excellence, not only within De La Rue but within our entire industry.'

The new facility is seen as a key milestone in De La Rue's business strategy, as the currency and authentication business grows significantly year on year and the identity business shows massive growth.

Order intake figures for the year are £533 million, said the company, which is a 16% growth in order intake from last year, with accelerated growth in the key areas of security features (up 60%), polymer substrates (up 23%), identity (up 36%) and PAT (up 97%).

www.delarue.com

Crypto-Anchors
(continued)

Highly secure

The crypto-anchors are described as highly secure because they are embedded in the product and consist of cryptographic mechanisms that provide unclonable identification, IBM said, adding that the technology would make counterfeiting 'nearly impossible.'

The first models could be made available in the next 18 months and within the next five years, advances in microfluidics, packaging platforms, cryptography, non-volatile memory and design will mean the technology could be widespread in the marketplace, IBM believes.

'We are saying in the next five years, crypto-anchors will halve the number of counterfeit goods that are linked to health and safety issues,' Head of IBM Research Andreas Kind said.

www.research.ibm.com

News in Brief

Veridos acquires E-Seek

Veridos – the identification and identity solutions provider headquartered in Berlin – recently announced the acquisition of E-Seek, a Californian company founded in 1999 that specialises in ID card verification technology. The acquisition, says Veridos, will strengthens its authentication portfolio and its presence in the North American market.

Veridos will specifically benefit from E-Seek's reading devices for government-issued driver's licenses and ID cards. These contain patented image capturing technology that ensures quick and accurate capture of security features and personal data contained on the card or in its barcode.

Veridos CEO Hans Wolfgang Kunz said: 'the need for fast and reliable verification of ID documents is increasing with the steadily rising numbers of travellers. Driver's licenses are often used as identification in North America, and E-Seek's devices improve the authentication process, especially at airports, for such documents. This acquisition brings together complementary products. E-Seek's hardware expertise and Veridos's proven software capabilities enable us to offer state-of-the-art ID card authentication solutions. The resulting synergies allows us to offer our customers an even broader portfolio of identity solutions.'

Chile Awards Tobacco Traceability Contract to SICPA

The Chilean Internal Revenue Service (Servicio de Impuestos Internos de Chile – SII) has awarded a contract for tobacco traceability to SICPA, following an international tender.

The contract will have a five-year duration and is valued at $45 million. It is eventually intended to trace about 780 million locally-produced and imported cigarette packs per year. The system will involve a mix of direct coding for cigarette packs locally produced for the domestic market and tax stamps for imported cigarette packs. Products for export will not be included in the system.

95% of the local tobacco market is provided by British American Tobacco (BAT), which owns a processing plant in Chile with over 20 production lines. According to 2015 information from BAT, the company produces about 1.2 billion cigarette packs yearly, of which 35% is exported.

Initial estimates by the SII put annual specific cigarette tax evasion at about CLP 188 billion annually (approx. $310 million), making the cost of the system only about 2.4% of the taxes currently being evaded.

5-Way Fluorescence from ANY

ANY Security Printing Company has developed a new security offset ink that shows five fluorescent features.

The penta-fluorescent ink emits blue/pink/greenish yellow fluorescence in long/medium/short wave UV respectively, plus anti-Stokes and infrared fluorescence. As a result, five fluorescent features can be obtained with one offset ink, providing added security for any printed document that utilises the technology.

ANY was formerly Hungary's state printer. It was privatised in 1993 and floated on the Budapest Stock Exchange in 2005, and is now the largest private security printer in Eastern and Central Europe. Its portfolio includes eID documents and issuance systems, passports, visas, stamps, tickets and cards for the government, financial and retail sectors. It also offers a wide range of security inks, of which the penta-fluorescent ink is the latest example.

Record Breaking Year for G+D

The global security technology group Giesecke+Devrient (G+D) has reported sales of €2.14 billion for 2017, a rise of 2% over 2016 and breaking a record for the second consecutive year. Adjusted earnings before interest and taxes (EBIT) increased by 4% to €130 million.

G+D Currency Technology passed the €1 billion revenue mark for the first time in its history. Revenue at €1.017 billion, accounting for nearly half of group turnover, was up by 10% compared with the previous year.

Sales in the other business units, all of which now operate as legally-independent companies, were €812 million for G+D Mobile Security (which specialises in electronic, digital and mobile payments), €167 million for Veridos (the identity business in which G+D has a 60% share), and €158 million for secunet (the IT security business).

The company has also announced the establishment of 'G+D Ventures', which serves as a company builder. Essentially this means that the unit picks up internal innovations (eg. prototypes built by advance52) and develops them into independent companies. Additionally, G+D Ventures also invests in external innovations and provides startups with access to the G+D network of experts.

G+D advance52 was launched last year to act as a catalyst for new digital technologies and business models within the company. It is a legally independent subsidiary that will help the subgroups to expand their digital business in the core areas of payment, identity and connectivity. The aim is for advance52 to develop new digital products to market readiness and then hand them over to the subsidiaries for marketing.

EC Takes New Measures Against Food Fraud

The European Commission (EC) has launched The Knowledge Centre for Food Fraud and Quality, a network to share information on food fraud and food quality issues. Operated by the EC's Joint Research Centre – it will bring together experts to 'support EU policymakers and national authorities by providing access to, and sharing up-to-date scientific knowledge' in this area.

Food fraud is becoming an increasing concern among governments and consumers alike. Last year, the EC proposed a series of measures to fight food fraud in the aftermath of the fipronil egg scandal in the Netherlands, which saw millions of eggs withdrawn from the market across Europe and hundreds of farms closed. Among the proposals was a mechanism for EU-wide risk monitoring and greater co-operation in the response to crises.

The new centre will coordinate market surveillance activities, operate an early-warning and information system and serve as a link point for information sources at the EC and member states. The EC says it will complement the existing EU Food Fraud Network, itself set up in the wake of the horsemeat scandal in 2013, by providing an interface between science and policy-making.

Surveillance will be conducted on the composition and sensory properties of food offered under the same packaging and branding on several markets across the EU.

The unit will also produce newsletters, interactive maps, databases and regular reports and will make this information publicly accessible.

How to Classify Security Features

By Martin Fürbach, Forensic Document Expert, University of Lausanne, Switzerland

This article discusses the classification of security features and how such features and the classifications thereof are influenced by the introduction of new techniques, communication and new methods of reproduction that are often used for counterfeiting. While these features can be classified according to different criteria (for example substrate based, printed, applied, preventing modification of entries (foils) and so on), the focus of this article is on classifications that are related to the level of examination.

Level of examination

The common classification in the literature and used in the industry is the level of skill of the person performing the verification. Based on the degree of skill required, the features are classified according to three or four categories. Public, inspection, forensic levels (and manufacturer in event of four levels) are often mentioned.

The first level (Level 1) is generally defined as able to be detected without tools by using visual or tactile features for rapid inspection in the field.

The second level (Level 2) is performed by trained inspectors using simple tools (magnifying glass, UV light and similar).

The third level (Level 3) is conducted by forensic specialists performing detailed examinations under laboratory conditions.

The fourth level can be done in collaboration with the manufacturer as definitive proof of authenticity.

Higher level – greater security?

Does the higher level of examination mean greater security? In general, the answer is yes, but there are exceptions. Complicated optical effects in Level 1 interactive features, for example, can be more difficult to imitate than can certain Level 2 features – eg. UV fibres present in paper that may be somewhat generic and more readily available.

In addition, this can be unique to a series of features for a specific document and country.

Visibility

A simple criterion that allows for the classification of features in two categories is based on whether or not they are visible to the naked eye. However, in practice, this is not clear for some features (eg. micro-text), as they are classified differently in the literature.

Confidentiality

One criterion for the classification of security features is whether the issuing authority has communicated them (or the opposite if their presence is part of classified information).

However, the general classification of security features is not definitively based on this criterion. It should be noted that the level of communication depends on the object / document and the issuing authorities.

For example, in the case of banknotes, the majority of central banks communicate at least some (public) security features; however, in the case of tax stamps or other documents, this is not as evident and even basic security features are either not disclosed at all or are communicated rather vaguely (such as information that a 'hologram is present' without further details).

Overt-covert

The classification according to two (overt and covert) or three (overt, semi-covert and covert) categories is also mentioned often in the literature and in technical standards.

For example, ' ISO 12931 – Performance criteria for authentication solutions used to combat counterfeiting of material goods' distinguishes between an overt authentication element – an authentication element that is detectable and verifiable by one or more of the human senses without recourse to a tool (other than everyday tools that correct imperfect human senses, such as spectacles or hearing aids) and a covert authentication element – an authentication element that is hidden from the human senses until the use of a tool by an informed person reveals it to their senses or else allows for the automated interpretation of the element.

Level of knowledge

The level of knowledge to detect security features is related to the level of examination; features at a higher level require greater knowledge. However, this is more valid for detection under laboratory conditions and begins to change slowly – some dedicated detectors of specific tags can be used by a person with minimal knowledge and can provide a binary response either in the form of visual or acoustic signals based on the presence or absence of the tag.

On the contrary, the complexity of some optical variable device (OVD) features might require more in-depth knowledge to evaluate whether the feature is genuine or not, and requires more than a simple 'present or absent' decision.

Devices needed for detection

Level 1 security features must be detectable without any tools and are based only on visual or tactile examination, while increasing levels require more sophisticated devices. For example, for Level 2 features, a magnifying glass or a UV lamp is sufficient, while Level 3 features will require a microscope and Level 4 an electron microscope.

Cost

The general understanding of the level of security has also been historically related to the increasing cost of the features (as well as the cost of detecting such features due to the cost of the devices, the training of personnel and the need for laboratory conditions and so on).

While Level 1 features are considered very inexpensive to detect and produce, Level 4 features are considered to require more expensive materials that are detected by very expensive machines.

But this is changing in two ways.

First, the sophistication and size of some Level 1 features means that their cost of production has become more relevant.

Second, the decreasing prices of portable detectors for taggants allows detection to be performed using devices that cost a fraction of the big laboratory machines used in the past; furthermore, the cost of training to use these devices and the time spent on detection are negligible.

Tobacco Products Directive (TPD)

The Tobacco Products Directive (see AN October 2017) requires security features on the individual packaging of cigarettes. The classification according to two categories (visible and invisible) in the TPD and later according to three categories (overt, semi-covert and covert) in the implementing decision has led to confusion regarding how to classify certain security features.

Challenges and problems related to classifications

While the classification of the security features can be a useful tool to understand the complexity of the security of documents bearing these features, it should not be overstated.

There are multiple reasons that classification may not be completely up to date, due to the evolution of the printing technologies, the evolution of counterfeiting and the evolution of detection.

Aim: exhaustive and exclusive classification?

The first misunderstanding is the tendency to classify one feature according to (only) one category, while ignoring the fact that some features can cover multiple levels.

For example, the ink used for printing the design elements may have specific infra-red or magnetic properties and contain taggants. Or in addition to the visual effect, a hologram contains nanotext and intentional errors in the nanotext, and so on.

In such cases, the features would fall into more than one category and even into all the categories in some cases. While the feature may be placed arbitrarily in one category, it may reduce its value in other areas – such as highlighted as a problem in the TPD.

By contrast, both ISO 12931 and ISO 18013 reflect this correctly and mention that, depending on the method of verification, one element may provide one or more security features that may apply to the same or to different categories.

Incorrect classification

Another example of classification being somewhat counterproductive is when the law requires certain features in certain categories, but the features are wrongly placed in a particular category.

This example pertains to the TPD implementing decision, as certain features should be in a different category from that in which they actually are – for example, visible fibres are placed in a semi-covert category, while UV fibres are placed in a covert category.

Moreover, this leads to the incorrect conclusion that features such as UV fibres have the same value as DNA or molecular taggants, as all are in the covert category. UV fibres of a particular colour can be common in different security papers used for different purposes (tax stamps, passports or banknotes in different countries), while a good molecular or DNA taggant will be completely unique and thus provide much greater security.

New printing techniques

Digital printing is creating a revolution in security printing in two ways. First, it decreases the value of conventional security features that could not be produced in the past without a particular printing technique.

An example is the case of serial numbers printed by letterpress. Historically, if a counterfeiter wanted to print a unique serial number they needed a letterpress numbering machine and, in many cases, specific fonts that were not available for commercial applications. While certain central banks still communicate the numbering of banknotes as a security feature, the value of this feature has decreased from Level 1 because these numbers can be imitated by other printing methods, such as electrophotography.

Second, another factor that is increasing the possibility of producing security features is the increased quality of digital printing and new ways of using the technology. Historically, digital printing was associated with the raster images created by isolated ‘dots’ of different colours. It was only possible to print guilloche or micro text on genuine documents via secure offset or intaglio printing.

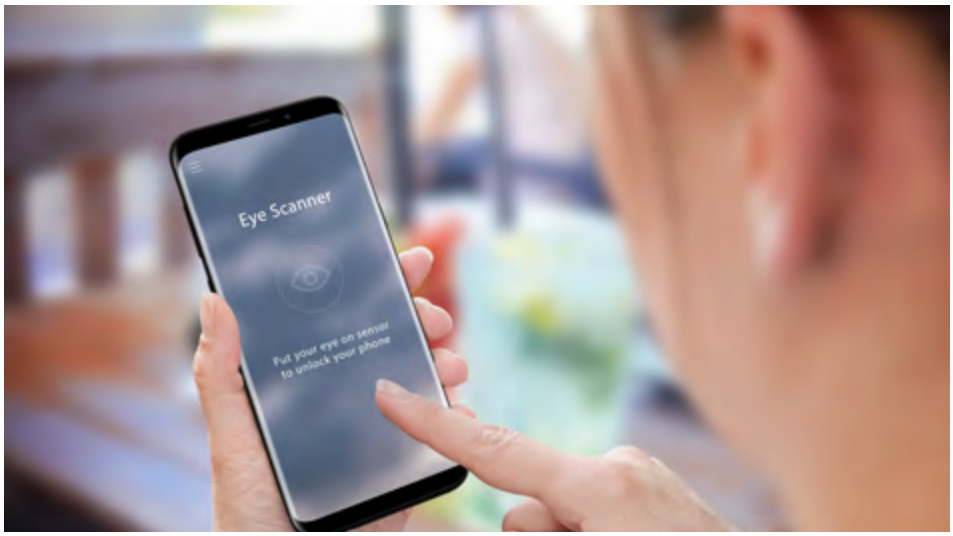
Now, however, digital printing is on its way to offering security printing applications beyond the well-established ones – personalisation of the documents (printing QR codes, numbers, names, photographs and alike), and completely secure documents such as tax stamps can be printed entirely digitally without a ‘typical raster’, including features that were reserved only for conventional printing techniques in past, such as micro text or a guilloche pattern.

Mobile authentication

Mobile authentication is revolutionising the way in which security features are verified, as it does not require expensive tools that are restricted to a small community of inspectors – anyone can download the application to a mobile phone. This allows for combining the verification of security features and information related to tracking and tracing. Multiple levels of information can be present as watermarks, fingerprints or steganography, and can be available to different users using different applications (public vs. inspection).

While this could theoretically already qualify as a Level 1 feature, at least in countries in which the penetration of mobile devices has reached almost the entire population, in todays definition of Level 1 (without tools, without devices), it is not possible.

How to Classify Security Features *(continued)*



Communication that is more open

In the past, communication about security features was very limited, if any communication was provided at all. For example, until the 1970s, central banks let people discover security features on banknotes on their own ways instead of describing them.

As security features, which were mainly substrate and design based at that time, began to be imitated by colour photocopy machines, along with the introduction of new interactive security features such as holograms and colour shifting inks, features generally began to be communicated in the form of brochures, and later in a more interactive form using websites and mobile applications. However, communication went even further.

Communication too far?

At present, even features that some experts still consider to be confidential (Level 3 – magnetism and infrared) are communicated as public features on central banks' websites.

Another problem related to confidentiality is that even if the issuing authority does not communicate features, this does not guarantee that features will remain secret. Not only does the issuing authority communicate, and disclose feature (eg. in the case of banknotes or passports), but in addition features are disclosed by the commercial databases that contain information about all countries.

Even when the confidential security features (such as the exact position of an error in repetitive microtext) are confidential and are not communicated, they can be reversed by the painstaking work of using a magnifying glass by passionate counterfeiters, who expect these features based on presence of these features in other documents.

Does this mean that, based on the 'shared knowledge', these features will start to shift to lower categories?

Criminals communicate as well

The internet facilitates communication not only with regard to genuine objects and desired communication from issuing authorities related to security features for public awareness, but also from another perspective – criminals.

Criminals have easier access to the information in various forms (discussion forums, video tutorials, the sharing of know-how related to materials and machines and so on). Recently, secret elements (such as the protection of banknotes against copying and latent steganography in documents) have their own pages on Wikipedia.

Commercial versus security printing gap

Historically, the introduction of OVDs to protect banknotes and passports was a breakthrough that was very difficult to imitate for a certain period due to the absence of commercial holography on the market, the small number of companies producing commercial holograms that could be misused, the high cost of production, and so on.

However, this is changing extremely quickly, and many security features are becoming easier to imitate as a result of the advances in commercial market.

Conclusion

Various possibilities for classifying security features do not enable easy classification, particularly in cases in which features are required to be present in particular categories, such as in TPD. This is even more complicated considering that classification has been used for dozens of years without reflecting changes in the production of security features, the detection thereof and the way in which they are communicated.

The table below shows the different security levels, how they are classified by the ISO12931, TPD, visibility etc. and the overlap between the different classifications.

Security Level/classification	1	2	3	4
	public	inspection	forensic	manufacturer
ISO 12931	overt	covert		
TPD	overt	semi-covert	covert	
Visibility	visible	invisible		
Confidentiality	public	confidential / secret		
Knowledge needed	(knowledge of presence)	minimum	advanced	specialized
Technical tools	(no tool)	simple tool	advanced tool	laboratory equipment
Example of tools	(eye or tactility)	magnifying glass, UV	microscope, magnetic reader	X-ray fluorescence, electron microscope
Example (printed feature)	design	microtext	magnetic properties	chemical composition of tag
Example (OVD)	visual effect	detail structure	nanotext	error in nanotext

Classification of the security features and the overlap between different categories.

Nanoparticles
(continued)

In this new development, nanotext, logos, barcodes, etc can be activated on the nanoparticles to emit strong colour when exposed to UV light. This process can be used for a variety of applications including labels, holograms for passports, vehicle registration number plates, licence discs and other applications. The activated luminescent areas can be detected using special electronic readers or microscopes with UV light.

The most significant features of this product are as follows:

- Bright photoluminescent colours such as red is produced on a nano scale area;
- Nanotexts, logos, barcodes, etc can be produced with laser activation of the nanoparticle;
- The nanoparticles can be printed or coated on any substrates, including polyester or paper, then activated by laser;
- The process can be produced in a roll to roll machines;
- The process can be developed further to produce nano RFID, serial numbers or for medical applications;
- The innovative process can be combined with conventional hologram processing to enhance authentication.

Idvac would be interested to collaborate with other partners to develop this process further.

www.idvac.co.uk

From the Archives

10 years ago...

Intelligent Wine Tracking System

eProvenance, a Franco-American technology firm, had developed a three-part tracking and authentication system for the wine industry aimed at preserving the quality of fine wines, tracing their origin and preventing pilfering and counterfeits.

The system was developed in response to concerns from wine companies in the Bordeaux region in France over the difficulty of ensuring the preservation of the quality of their wines during handling, transportation and distribution. Maintaining temperatures in a reasonable range during shipment and storage plays an important part in preserving quality, but there is often no record of variations of temperatures after the wine has left the wine producer's cellars.

The first part of the system therefore involved semi-active radio frequency identification (RFID) tags, which were placed inside each case and enabled wine producers and distributors to monitor and log ambient temperatures three times a day.

Second was a passive RFID tag with a unique code, applied to the base of each bottle to enable each to be tracked, and to prevent pilfering.

And third was a proprietary tamper-proof neck seal with a covert code, which could be read by the eProvenance authenticator and was designed to authenticate the bottle and its contents.

Each of the three components were linked with their unique identification numbers in a high-speed, online, encrypted database. According to eProvenance, 'this combined data creates an ePedigree for each bottle of fine wine, which consists of authentication data from the château, shipment data and temperature records'.

The automated monitoring system cost €5,000 a month for five months, excluding hardware and tags.

eProvenance continues to provide intelligent tracking services to the wine industry and has expanded its product offering as a global service to monitor and analyse shipment conditions during transport and storage of, for example, fine art and other items of value.

20 years ago...

EMI Selects DOVIDs for Euro

The European Monetary Institute (EMI), responsible for the design of the new euro currency, had decided that the primary overt authentication feature on banknotes would be a diffractive optically variable image device (DOVID) foil stripe on lower denominations and a DOVID foil patch on denominations of €50 and over. Although no formal announcement was made, the EMI selected a design by French company Hologram Industries (HI) for the patch and a design by Swiss company OVD Kinegram for the stripe.

The EMI would not provide any details about the DOVIDs and both companies were unable to discuss this contract. It was understood that the details of the supply agreements were still being worked out. Production was to be contracted separately from the design and mastering, so the originators would be required to assign rights in their designs to the EMI in return for a royalty on the DOVIDs produced.

The central bank in each of the 11 countries participating in the euro currency was free to choose its currency printer and foil supplier from those approved by the EMI. Several European embossed foil manufacturers ran production samples for evaluation by the EMI, although informed observers estimated that few had adequately secure plant and audit procedures to meet the required quality standards for the production volumes and security standards. At the time, those considered likely to qualify were KURZ, which already manufactured Kinegrams as sub-contractor for the deutschmark and other currencies, and De La Rue Holographics, which had produced DOVIDs for several currencies printed by its parent company.

In 2002 the first euro series was introduced with each banknote carrying a DOVID. This was followed in 2013 with the introduction of the first denomination of the second euro series of banknotes called *Europa*, with the introduction of the new €5 note. This was followed by the 10, 20 and 50 denominations, released in each of the subsequent years.

The final two new Europa series denominations (the €100 and €200 notes), to be issued simultaneously in 2019, will also incorporate a DOVID stripe feature.

India's Authentication Forum 2018

India's second two-day international authentication conference and exhibition – The Authentication Forum 2018 – held in New Delhi in March and organised by the Authentication Solution Providers' Association (ASPA), proved to be a huge success, providing an insightful programme of presentations and panel discussions.

A high profile panel of experts including government authorities and technology specialists came together to mark the launch of the second forum, which was inaugurated by Suresh Prabhu, Union Minister, Ministry of Commerce & Industry & Civil Aviation, Government of India.

In his inaugural address, Prabhu reiterated the government's resolve to deal harshly with the rising menace of counterfeiting. 'We are going to make a very modern Intellectual Property Rights (IPR) era in India and that would lead to creating people investing into the brand and that will lead to a knowledge economy which in turn will make India a far better and developed place,' he said.

In addition to the Union Minister, dignitaries including the Registrar General and representatives of Protection of Plant Varieties and Farmers Right Authority, Central Board of Excise & Customs, Hyundai, Society of Automobile Manufacturers (SIAM), Ernst & Young, KPMG, Hero Motor Corp, FMC Corporation, Pesticide Manufacturers Association of India (PMFAI), Anand & Anand and others also shared their viewpoints at the summit.

The President of ASPA, U K Gupta said: 'counterfeiting is increasing globally. In India also, the problem is growing with an alarming rate of almost 44% per year. As per the industry body FICCI-CASCADE, the Indian government incurred a loss of Rs 26,190 crores in fiscal year 2011-12 due to counterfeiting activity, which increased to Rs 39,239 crores in 2013-14, a growth of 49.8% in two years. The market for fakes are on the constant rise and has surpassed over Rs 40,000 crore in the organised sector alone, as law enforcement remains weak and fraudsters freely make inroads into the market.'

Day One of the summit program included three panel discussion – The Role of Government and Industry in Fighting Fakes and Protecting Consumers, Understanding the 5Ws of Counterfeiting, and Engaging Consumers in the Fight against Counterfeiting.

In the last session of the day, companies including Holostik, Manipal Technologies and Rolling Optics delivered presentations on current authentication solutions against counterfeiting.

The second day of the summit started with case studies from brand owners, sharing their perspectives. They included Dr Bakul Joshi, Brand Protection Expert, FMC Corporation with a case study on protecting agrochemicals products and Naveen Chauhan, Head of Sales & Marketing (Parts Business) on the automotive industry's perspective. This was followed by the pharma perspective presented by Sourav Mitra, Associate Vice-President Packaging Strategy – OSD.

The event also witnessed a dedicated session on the future of anti-counterfeiting technologies, including blockchain, NFC, optical and offline authentication. The audience also got the chance to learn about the importance of branding, IPR and effective intelligence.

The forum ended with 'The Big Debate: Global Growth of Counterfeiting Trade – Why is it Increasing – Lack of Intent, of Action or of Awareness?'

www.aspaglobal.com

RECONNAISSANCE AUTHENTICATION NEWS®

Publisher: Reconnaissance International Ltd.
Editor: Mark Deakes (right).
Contributors: Martin Furbach, Astrid Mitchell.

Annual subscription rate: £575 *plus postage*

Subscribers to Holography News, Tax Stamp News or ID & Secure Document News: 20% discount. Ask about multiple/corporate subscriptions.

The editorial team welcomes your news, contributions and comments. Please send these to publications@reconnaissance-intl.com

10 Windmill Business Village, Brooklands Close, Sunbury, TW16 7DY, UK
Tel: +44 (0)1932 785 680; Fax: +44 (0)1932 780 790

www.authentication-news.com

ISSN 1368-857X

Events

21–24 MAY 2018
THE BANKNOTE CONFERENCE
Dallas, TX, USA
www.banknoteconference.com

6–8 JUNE 2018
WCO IT CONFERENCE AND EXHIBITION
Lima, Peru
www.wcoomd.org

11–13 JUNE 2018
HIGH SECURITY PRINTING LATIN AMERICA
Dominican Republic
www.hsp-latinamerica.com

25–27 JUNE 2018
SECURITY DOCUMENT WORLD
London, UK
www.sdwexpo.com

25-27 SEPTEMBER 2018
LABELEXPO AMERICAS
Chicago, IL, USA
www.labelexpo-americas.com