



## WCO's IPM Platform Moves into a New Phase



**The World Customs Organisation (WCO) has advised that it continues to see evidence that illicit trade in all its forms is growing exponentially, and that if the fight against illicit trade is to have any success, all stakeholders must work together, harnessing all available technologies, in a systemic response to a scourge that is just getting stronger.**

With this need for a multi-stakeholder systemic response in mind, the WCO is extending its IPM anti-counterfeiting platform to a broader range of stakeholders, situated outside of the organisation's scope. It will do this by transferring the ownership and further development of IPM to PSS, a wholly owned subsidiary of Swiss company TechTrace SA, the long-standing technology provider behind IPM.

IPM is the only global security solution gateway to allow customs officers to verify the authenticity of products online, by acting as a real-time communication hub between brand owners and customs officers. Interfaced with IPM is IPM Connected, a global network of track and trace and authentication solutions, provided by IPM's 26 security solution partners.

The intention of the WCO is to make IPM available to all relevant agencies and governments active in the fight against illicit trade. Currently, the platform is used by brand owners from over 14 product sectors (including food, beverages, pharma and tobacco), as well as customs officers in over 90 countries. The WCO also has IPM partnership agreements with 14 international organisations.

'WCO has achieved significant progress in meeting the challenges posed by illicit trade. IPM is the only global tool in a war which requires us to be ever more innovative. It is time for IPM to move to a new phase which will enable broader international cooperation which is crucial to our continued success,' said Secretary General of the WCO, Kunio Mikuriya.

According to Adam Blackwell, Chair of the Advisory Board of TechTrace, 'while this is a daunting task, TechTrace is committed to energetically responding to the opportunity being given to it by the WCO.'

Continued on page 2 >

## Authentication for Luxury Fashion

**Entrupy – a US start-up company launched last year – has introduced an on-demand authentication portable scanning device solution for the luxury fashion industry that enables businesses and consumers to authenticate anytime, anywhere using a mobile app, Apple smartphone and portable device.**

The company has initially focussed on second-hand resellers of luxury and designer items, particularly handbags, because of the growing risk of counterfeits in purchasing authentic luxury goods, and in particular from online retailers.

Entrupy provides scalable technology capable of authenticating luxury products from brands such as Louis Vuitton, Hermes and Chanel, among others.

The technology works by taking microscopic photographs of different areas of an item and uses artificial intelligence (AI) and machine learning algorithms to analyse the images. The images are then compared to database images to determine authenticity.

The person wishing to authenticate the item simply places the Entrupy device directly on the item (like a luxury handbag), opens the Entrupy app on their smartphone or tablet and follows the onscreen prompts in the app to take images. Entrupy's AI algorithms analyse the images to determine authenticity and provide real-time results.

The device works on various materials ranging from canvas and leather to metal and wood, and has an authentication accuracy of over 96.4%, while producing results in seconds.

Continued on page 2 >

## Inside this Issue

- 1 WCO's IPM Platform Moves into a New Phase
- 1 Authentication for Luxury Fashion
- 2 Packaging To Use Artificial Intelligence for Authentication
- 3 News in Brief
- 4 The World's First Iris Verification ID Card Solution
- 5 Orell Füssli Unveils SPECTRAL
- 6 Printing Beyond Colour – White Inks
- 7 From the Archives
- 8 Arjo Solutions Partners with Epson to Launch DOCS

# Packaging To Use Artificial Intelligence for Authentication



Swedish company AR Packaging has developed a process to print copy resistant and random security markers combined with inline variable QR codes directly onto packaging. The process is called *FUTECO*, and the company has signed an exclusive strategic partnership with Paris-based artificial intelligence (AI) company Cypheme SAS to develop the commercial anti-counterfeit potential of the technology.

Cypheme provides AI-powered systems capable of recognising a printed product's packaging marker with a neural network, using only a mobile phone camera. The technology enables a fast and easy way, accessible to anyone anywhere, to verify the authenticity of the products using the solution, it says.

According to both companies, the combination of market insight and the Futeco concept will provide anti-counterfeit and traceability features, together with high efficiency printing processes.

Harald Schulz, President and CEO of AR Packaging, commented, 'I am pleased to add another new feature to our wide portfolio of innovative packaging solutions in line with our set strategy.'

'The Futeco security concept offers our customers a unique solution to counterfeiting detection and thereby enables them to achieve competitive and economic advantages in the market place.'

Hugo Garcia-Cotte, CEO of Cypheme, added, 'this partnership allows us to boost our technology, giving it new forms that will fit new types of products and new volumes.'

Under the terms of the strategic partnership, AR Packaging will acquire an equity stake in Cypheme.

[www.ar-packaging.com](http://www.ar-packaging.com)

[www.cypheme.com](http://www.cypheme.com)

## WCO's IPM *(continued)*

'We look forward to fully developing the necessary networks, alliances and products to forcefully respond to the challenges of the illicit economy'.

In order to ensure a smooth transition, the transfer will be gradual, with a handover scheduled to be completed over the coming months.

For more information on TechTrace contact Hans Schwab, Managing Director of TechTrace, [hans.schwab@techtrace.com](mailto:hans.schwab@techtrace.com)

## Authentication for Luxury Fashion *(continued)*



The Entrupy authentication reader.

The accuracy of the analysis is driven by the database, which uses about 150 samples from each real product, with additional samples marginally improving the accuracy for that brand – for example, the device has accuracy ratings of above 99% for Hermès and Louis Vuitton handbags.

The analysis also takes into account workmanship, processes and specs such as how, where and when authentic goods were made, making the system hard to forge.

In the future, the company hopes to move onto authenticating other physical products and items.

[www.entrupy.com](http://www.entrupy.com)

# News in Brief

## Optaglio Invests in Forensic Research

Optaglio – the Czech-based surface relief optical security device and hologram producer – has established a new research centre focused on forensic aspects of anti-counterfeit protection technologies for different types of documents.

This new centre will work as a separate unit closely connected to Optaglio Labs. It is equipped with a broad range of technical capabilities that will simulate different types of counterfeiting attacks against documents, such as the removal of protective elements.

The core focus of the research centre will be on strategies for protection against such attacks and the development of new technologies. All new anti-counterfeit measures and developments will undergo rigorous production testing to ensure they are robust and durable for their application. The centre is partly subsidised by EU funds.

The company has also announced a collaboration programme with university departments and a commercial partner to develop the next generation of e-beam lithography systems, ensuring optical security devices remain many steps ahead of the counterfeiters.

Since 1998, Optaglio invested significant effort and resources into the development of e-beam technology, launching many new innovations, holographic features and visual effects. According to Luboš Malák, Optaglio's e-beam lithography divisional manager, 'if we want to be a provider that can guarantee anti-counterfeiting technologies for our customers, we are obliged to invest into innovations for the long-term.'

Key parts of the development will be undertaken by the company's in-house research team, which will define detailed tasks and specifications for the hardware, technical requirements, sampling and testing. Other stakeholders involved in the project include undisclosed university departments and the (un-named) commercial organisation.

## DLR Plans Pay Off

De La Rue's restructuring plans, announced last year, appear to be paying off – with both sales and profits in 2016/17 rising.

The company reported annual sales up by 2% to £461.7 million. Pre-tax profit was 6% higher at £58.2 million. Both figures are on a like-for-like basis, and exclude the cash processing business that De La Rue sold last May.

Banknote printing accounted for £350.6 million of sales. The company produced 7.1 billion notes during the year, in line with 2015. Banknote paper volumes increased by 18% to 11,800 tonnes – a seven year high.

The Identity Solutions business printed 13.7 million passports in the year and generated sales of £80.6 million. The Product Authentication business, which delivers brand protection and tax stamp solutions, generated profits of £9 million on sales of £34.6 million, up by 29% and 20% respectively.

The company is in the process of streamlining its global production footprint, as part of its 'Optimise & Flex' programme. Restructuring the printing operations is on track to generate £13 million in savings annually from 2018.

It's 'Invest & Build programme', meanwhile, has seen accelerated product development, volumes for its *Safeguard*<sup>®</sup> polymer substrate nearly quadrupling to 380 tonnes, the acquisition of DuPont Authentication (the company's first in 14 years – see AN December 2016) to broaden its portfolio of security features, and the opening of a Centre of Excellence for security print in Malta (see AN April 2017).

## Nanotech Goes for Growth

Vancouver-based Nanotech Security Corp – a specialist in the design and production of advanced banknote and commercial branding authentication products – has secured \$12 million in funding to help grow the company.

Nanotech creates nano-optical devices with vivid colour images. In 2014, it bought Fortress Optical Features, which was established by the Bank of Canada to develop and produce thin film interference filters using vacuum deposition technology, from which to make colour shift windowed threads for banknotes.

Last year Nanotech signed a memorandum of understanding (MOU) to collaborate in the production of new colour shifting security features in optical thin film (OTF) with Hueck Folien. More recently, it signed another MOU with Zhongchao Special Security Technology (ZSST), a division of China Banknote Printing and Minting Corporation.

Net proceeds from the finance offering will be used to simplify and improve Nanotech's capital structure; increase production capacity for its *KolourOptik*<sup>®</sup> images and optical thin film; and strengthen the balance sheet for working capital and general corporate initiatives.

Nanotech CEO Doug Blakeway commented that 'this financing puts Nanotech in a very good position to execute growth opportunities that could accelerate the growth of the company significantly over the near term. We are excited about contract prospects across several end-markets including our unique nano-optical image technology, as well as our commercially proven thin film colour-shifting technology.'

## OpSec Goes Mobile

OpSec Security has announced the extension of its mobile *InSight* platform to include authentication of advanced optical security images. OpSec InSight provides brand owners and governments with end-to-end visibility of supply chain and distribution operations of their products' life cycle, from conception to consumer, enabling them to manoeuvre through various reports and dashboards with actionable information detailing authentication, serialisation, online brand protection, consumer engagement, and trademark management.

As a further enhancement, the company has developed a series of mobile authentication technologies that bring the convenience and ease of authentication and access to smartphone users throughout the supply chain – brand owners, enforcement professionals, and consumers.

The new mobile authentication technologies will work with OpSec's entire portfolio of overt, covert and digital security technologies. The combination of these in a single authentication device will provide stakeholders with immediate access to product information and significantly raise the barrier of entry for counterfeits and overproduction, says the company.

In a separate announcement, OpSec also announced the next generation of *Trademark InSight* with an improved suite of web-based licensing tools. These include agreement and royalty management, secure digital asset management, and product approval workflows.

Users also have the ability to grant organisational rights by properties, products, channels, regions, and other program-defined attributes.

# The World's First Iris Verification ID Card Solution



HD Barcode LLC is a solutions developer, integrator, and provider of proprietary barcoding technologies. It has partnered with IriTech Inc, a biometric technology provider, to introduce the world's first ID card – *HD IrisCheck™* – with the ability to store biometric data, photo, and information about an individual into one code, called the *HD Barcode™*.

Unlike public codes that can be created by anyone, such as QR codes, the HD Barcode requires a secure code generator which remains with the customer. This ensures those with the ability to read HD Barcodes may not create or alter code data.

## How does it work?

Each organisation, institution, or manufacturer has their own unique code generator and authorisation key for decrypting HD Barcodes. The separation of generating and decrypting printed codes ensures organisations can positively ID members, visitors and other authorised individuals, while ensuring unauthorised personnel are not able to alter code data.

The individual's iris data, photo, and related text, such as position held, clearances, emergency medical information etc., is captured and embedded in the HD Barcode for multiple levels of positive identification and accessible without a database lookup or internet connection. This ensures information is readily available when there's a loss of communication and/or power failure.

To create the ID card, the individual places the camera in front of one of their eyes, which allows the software to capture and convert the iris information into a proprietary digital format.

The system has the advantage of being able to capture iris image information even if the image is affected by eye glasses, contact lenses, tears, eyelids, or eyelashes. Iritech's software is able to operate with no discernible performance degradation as long as at least 50% of the iris image sectors are good at the time of enrolment and at least 25% are good at the time of identification.

The individual's photo and relevant content are combined with their iris details and sent to the 'HD Barcode Generator' and converted into a printable 2D HD Barcode. The ID card is then printed with human readable content along with their unique and secure code, on one or both sides of the card, using existing printing processes.

## How is it read?

The HD Barcode can be read with devices such as an android smartphone, PC, or custom terminal which are designed to detect metadata embedded within the HD Barcode to determine its authenticity. This embedded security key can be changed from time to time and multiple keys can be utilised for different users.

When the data is confirmed, the reader device will decrypt and display the information contained within the HD Barcode. The companies say there are no possible 'backdoor' methods of bypassing the authentication procedures.

Devices can be time stamped and only usable during specific periods of time. Authorised personnel can also be issued an ID card with a separate HD barcode that must be scanned before the application is activated and usable. This prevents reader devices from becoming compromised in the event they are lost or stolen.

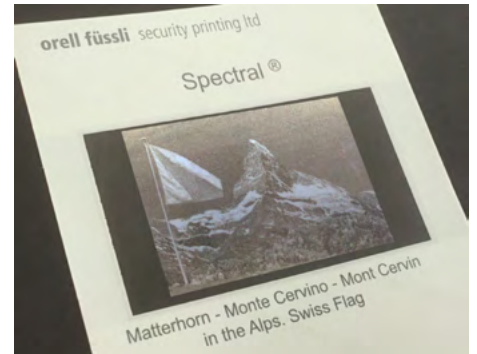
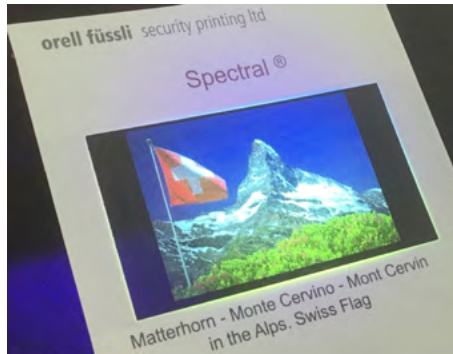
Once the individual's HD Barcode has been decoded, their identification can be further verified by scanning their iris using Iritech's approved camera (*IriShield™* scanner) and partnered software. A one-to-one comparison between their scanned iris and stored biometric data is performed, thus confirming the person's identity.

[www.hdbarcode.com](http://www.hdbarcode.com)

[www.IriTech.com](http://www.IriTech.com)



# Orell Füssli Unveils SPECTRAL



Left: On a light background, the window is transparent. Middle: Under UV light, a photo-realistic image appears. Right: On dark background, a grayscale image is visible.

**Swiss based Orell Füssli Security Printing Ltd – a manufacturer and services provider of banknotes, identification documents and systems, and value transfer documents – recently unveiled at this year’s Currency Conference, in Kuala Lumpur, a new security feature for banknote windows called SPECTRAL®.**

Orell Füssli Security Printing dates back to the 16th century and is a well-known manufacturer of banknotes, particularly Swiss banknotes for which it has won numerous accolades.

In addition the company also provides security technologies and solutions for identification documents and systems, and secure documents.

The company has also been actively innovating with the development of its latest high security banknote window feature – SPECTRAL. This comprises photo-realistic images printed in offset within banknote windows using UV fluorescent inks that are only visible under UV light.

The UV fluorescent inks absorb light in the UV wavelength range and re-emit part of the light into the visible wavelength range, therefore becoming visible to the naked eye.

The name Spectral is derived from the two image aspects of the feature (see above): the spectrum as a full colour image as seen under UV light, and the ghostly or relating to a spectre, as a grayscale ghost-image as observed on a dark background.

## How does it work?

Under standard daylight illumination conditions, the inks are transparent – as shown above, which depicts a transparent window of a sample banknote printed on *Guardian®* polymer banknote substrate.

When the substrate is illuminated with UV light, a full colour image appears in the window, almost akin to an overt level 1 type feature.

A further grayscale image (or ghost image) becomes visible under standard daylight illumination when the window is placed on a dark background, as the transparent inks scatter the light.

To ensure the UV fluorescent effect produces the most colourful images and does not diminish due to ink superposition (quenching effect) and/or ink contamination during the offset printing process, a patented half-toning method is used that relies on diagonally orientated screening.

Mathematical models are also used to map the visible colours into the range of printable colours with the limited colour set of UV inks.

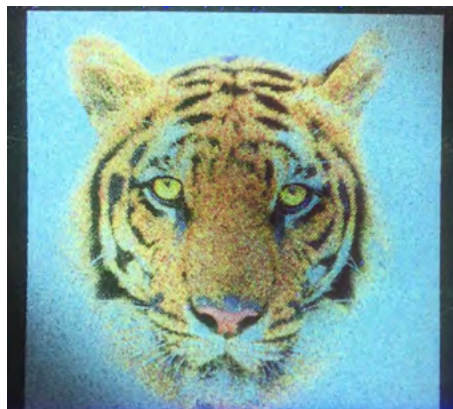
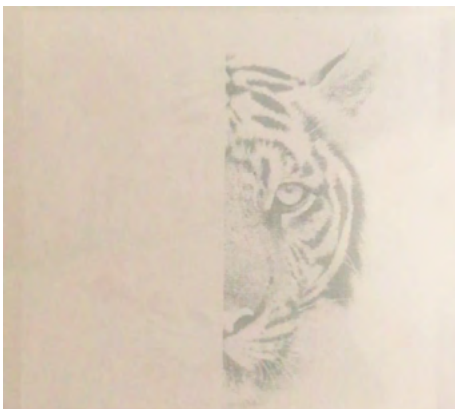
## Design opportunities

According to the company, Spectral ‘opens up’ a myriad of design opportunities for the banknote designer and also the possibility to enhance security.

For example, the banknote designer may integrate the feature by printing parts of an image in dark visible inks on a light background. Below shows half of an image printed in dark visible ink which, when illuminated under UV, reveals a photo realistic image in full colour.

Meanwhile, the below picture on the right shows the same image under standard daylight conditions on a dark background which reveals a whole image as ghost image.

[www.ofs.ch](http://www.ofs.ch)



Left: On light background, an image is visible in dark colour. Middle: Under UV light, a photo-realistic image appears. Right: On dark background, the complete tiger is visible.

# Printing Beyond Colour – White Inks

By Alan Hodgson

This series of articles that examines technologies for ‘printing beyond colour’ moves to a conclusion by considering the threats and opportunities raised by the development of white inkjet inks. The purpose of this article is to outline some of the recent developments in this field and make you aware of their capabilities in the wrong hands. It also gives an overview of the where white ink digital printers are appearing, with a particular emphasis on their characteristics.

And as a final conclusion to this series readers should also note that it contains a number of examples where looking outside of our industry for technologies is worthwhile – casting a ‘Wider Eye’ on the surrounding technological landscape.

## White inks – an overview

In the printing industry, clear or white toners are often used to produce low security digital ‘watermarks’ that cannot be copied or scanned but can be observed by a human reader. This capability would not go unnoticed by the counterfeiters and a good example of this was given at a workshop at the High Security Printing™ EMEA conference in 2016. It was shown that it is possible to produce facsimile watermarks in paper through page splitting and screen printing with a white ink.

White inks have been available for conventional printing presses for many years. They are, however, a relatively recent addition to digital printing. The key point to note here is that over the last few years a number of industries have had a requirement for white inkjet inks.

As a result these are now available on a variety of printer sizes, resulting in widespread availability for both legitimate manufacture and illicit copying or alteration.

In the early days of digital colour printing, almost all available printers had four colours; cyan, magenta, yellow and black (CMYK). This was later extended in some specialist printers to six or more channels to encompass spot colours or to increase the printable colour gamut.

These options also enabled the incorporation of security features like fluorescent inks in some passport printers.

As noted earlier in this series, the concept became further extended by the provision of clear inks (see AN March 2017). This was extended to white inks somewhat later due to the difficulties in formulating stable inks of suitable whiteness and covering power.



However, relatively recent developments in ink manufacture and inkjet print head design have solved these issues.

## Printing ‘difficult’ inkjet inks

Inkjet print heads for commercial, office and desktop printing are complex devices designed to minimise print artefacts (see AN March 2016).

To achieve this, the inks are formulated as either a dye solution or a dispersion of very small pigment particles. And this is the problem with the formulation of white inks.

An example serves to illustrate this in a security printing context. Titanium dioxide is sold as CI Pigment White 6 for the formulation of printing inks. However, if it is milled small enough for typical inkjet applications it becomes almost colourless.

This is the technology used in the ‘inkjet printed hologram’ work at the University of St Petersburg (as featured in the January 2016 issue of *Authentication News*® sister publication *Holography News*®), which utilises a finely milled titanium dioxide pigment to produce a colourless inkjet printable ink to render a pre-printed diffraction pattern visible.

The overall message here is that larger pigment particles produce a more opaque white ink. The problem has been that these tend to clog the print head, resulting in uneven printing.

However, new generations of print heads, particularly those aimed at technologies like printed electronics (see AN February 2016) together with advances in ink formulation, have recently made the inkjet printing of white ink a commercial reality

## White inks in industrial settings

It is instructive to look where these white ink printers are being implemented for two reasons. First it shows the type of capability being available for industrial scale use. Second, it provides an illustration of the systems that could be used for illicit copying or alteration.

There are a wide range of printer types available with white ink. Most use UV cured ink, but in addition there are water based solutions available. This allows the technology to take in opaque and transparent polymers and paper too.

There are a number of flatbed UV cure solutions available on a variety of scales. At the lower end of the scale is the *Axzyra Apache* (below) with a print area of 450mm<sup>2</sup>.



The Axzyra Apache 4545.

10 years ago...

## Kodak Launches 'Virtual Fortress' of Security Features

*Authentication News*® reported that prepress, imaging and digital print specialist Eastman Kodak Company had launched Kodak Security Solutions – a range of products and services targeted at both document and product security – which it described as a 'virtual fortress to help the world fend off counterfeiters.

At the heart of the range was the *Kodak Traceless*™ system, comprising taggants and proprietary handheld readers. This system was originally developed by Creo and launched in October 2004. In 2005 Creo was acquired by Kodak.

Traceless is a synthetic mineral taggant supplied as a powder that can be mixed with inks, toners, varnishes and other items for both analogue and digital printing, as well as paper pulp, plastics, powders, pigments, liquids and textiles. It has a detectable concentration of under two parts per million and a life of 100 years, and can be detected only with the Traceless reader – ie. not by chemical or spectroscopic analysis. Line of sight reading is required, but not contact, enabling the marker to be detected under surfaces such as glass or laminates.

Two versions of Traceless were made available. In one, the reader would detect the presence or absence of the compound.

Alternatively, the random pattern of the particles on the surface of the item to which it had been applied could be recorded and converted into a number unique to the product. This number could be printed back onto the item and/or recorded in a secure database. The reader would then match the distribution of particles against the printed code, or the same code stored in the database.

In addition to Traceless, the company outlined that its covert technologies included other markers, as well as digital watermarking and magnetic ink character recognition (MICR). It also offered a number of overt security technologies, including watermarks, microprint, 'raised' print and variable data.

The company targeted a number of sectors including pharmaceuticals, apparel, cosmetics, ID documents, tax stamps, tickets, food and beverages, and reported that several of the most prestigious wineries in Napa Valley in California were now using its technology in the labels of their premium wines.

*Today Kodak's portfolio of Traceless products has expanded to include thermal transfer ribbon with the Kodak Traceless Anywhere System.*

In addition to CMYK and white these units can also print clear inks (see AN March 2017) and tactile features (see AN April 2016). Larger scale units than this are used to print directly onto transparent interior doors to add signage on a white background.

The label printing industry is also a user of white ink, resulting in the availability of narrow width roll-to-roll UV cure solutions onto polymer substrates.

Used for premium quality labels, this industry has also evolved colour management solutions involving white printed over colour. This industry too uses white inks for tactile features.

The final example is given by sheet based proofing printers such as the Epson *Stylus® Pro WT7900*. Epson use a water based ink, giving full compatibility with paper based substrates from a relatively small printing engine. Screen printing with white ink may not be the only way in which watermarks may be illicitly duplicated.

### Bespoke solutions for mobile electronics

This is an example where casting a 'Wider Eye' over developments outside our community is of benefit. Mobile devices such as smartphones have a coloured (commonly white, black or metallic) bezel around the display area, usually with a brand name incorporated. Often manufactured out in Asia, these bezels hide the edge wiring of the display and are now being printed using inkjet technology.

There is market demand for white bezel solutions from a number of manufacturers, and for copies of these. These manufacturers also have very specific colour and opacity requirements, often to tight tolerance.

This is resulting in the development of new ink and printer solutions from their suppliers for transparent materials that include polycarbonate.

### Threat or opportunity?

As should be clear from the above summary, these capabilities are now widely available. The technologies are scalable and still being developed. The knowledge of how to utilise them will also be widespread.

We should certainly consider this widespread availability of white ink capability as a threat to some established security features. There are solutions capable of printing onto paper and established polymer substrates such as polycarbonate.

The fact that inkjet takes this capability into digital printing must ease the workflow constraints on illicit copying and manufacture.

But equally we should not ignore the potential for an opportunity to develop novel features. There is now the opportunity to add an additional colour to inkjet printing solutions that could raise the bar to illicit copying. These could incorporate some of the additional elements outlined below.

Future developments may also bring on more opportunities, probably incorporating optical features. The mobile electronics industry is already incorporating printed light reflecting layers under white bezels. White ink layers of varying opacity also make excellent printed optical diffusers.

These same inkjet printing engines are capable of a wider range of colorant options. Metallic looking inks are already commonplace and some have some semblance of opalescent features.

Metallic appearance inks are worthy of a whole new article for the future. Casting the 'Wider Eye' over the materials appearance community would also be worthwhile, as the automotive industry is conducting some interesting work in this area.

### In summary

White inks and suitable printers now have widespread availability. The technology scales to metallic colorants and tactile features too. We should consider this as both a threat and an opportunity.

Steve Woods, Managing Director of Axzyra told me that 'the recent development of inks that keep the cost and complexity of small units at a cost point suitable for start-ups and small home businesses have been a real bonus.'

'Indeed, metallic inks fall into the same category. Ink coverage at higher speeds on single pass with white and colour is also a big consideration.'

# Arjo Solutions Partners with Epson to Launch DOCS

Arjo Solutions – part of the Impala group, and a provider of physical and digital identification, authentication and traceability products and materials – has announced the launch of **DOCS (Document Certification by Signoptic®)** in partnership with Epson, a leading provider of digital printing, visual communication, wearables and robotic systems. The DOCS solution utilises the intrinsic material of the document to produce a digital fingerprint that enables both document identification and the authenticity of the variable data to be validated using a smartphone application.

DOCS uses the biometric information of the document by using Signoptic technology. This innovative technology is based on a vision system that enables the conversion of a document's texture into a unique digital signature (sometimes referred to as a fingerprint or materials biometrics) by use of a proprietary algorithm. As the signature is generated from random elements of the document itself, the solution is similar to the Automated Fingerprint System Identification (AFIS) system for a human being.

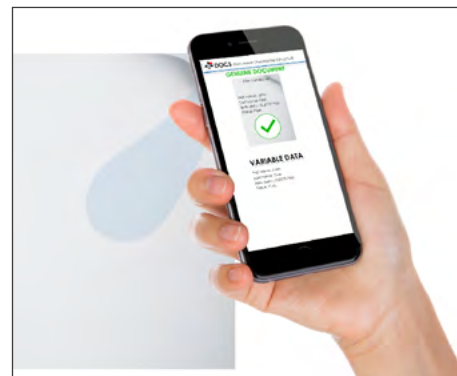
DOCS enables document authenticity to be checked and traced during its validity period and after, without any additional features or design modifications. In addition, due to the unique link between the document's Signoptic signature and its variable data, the system can also detect falsification attempts.

## Personalisation

DOCS is suitable for all types of personalisation, and the registration of each document can be carried out either by a vision system on a production line, or by a professional office scanner (Epson) in a decentralised environment.

The document authentication verification process can then be undertaken via the same scanner or by using a simple smartphone application (Android or IOS).

Using DOCS, governments, certifying organisations and administrations have a solution that allows detection of blank stolen documents, by highlighting all authentic documents falsifications and identifying all reproductions.



Arjo Solutions was formerly part of the French papermaker Arjowiggins Security, which acquired Signoptic in 2011. It was hived off as a separate subsidiary, along with its sister company Arjo Systems (specialists in ID technologies) and sold to the asset management company Impala in 2015 (see AN May 2015). Its main markets are brand and revenue protection.

[www.arjo-solutions.com](http://www.arjo-solutions.com)

[www.global.epson.com](http://www.global.epson.com)

## RECONNAISSANCE AUTHENTICATION NEWS®

**Publisher:** Reconnaissance International Ltd.  
**Editor:** Mark Deakes (right).  
**Contributors:** Alan Hodgson, Astrid Mitchell



Annual subscription rate: £575 plus £25 per year for 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](mailto: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](http://www.authentication-news.com)

No part of this publication may be reproduced, stored in a retrieval system or translated in any form or by any means – electronic, mechanical, photocopying, recording or otherwise – without the prior permission of the publishers. While every effort has been made to check the information given in this publication, the publishers cannot accept any responsibility for any loss or damage arising out of, or caused by the use of, such information. Opinions expressed in Authentication News are those of the individual authors and not necessarily those of the publisher.

COPYRIGHT 2017. ALL RIGHTS RESERVED

## Events

**26–28 JUNE 2017**

**SDW 2017**  
London, UK  
[www.sdwexpo.com](http://www.sdwexpo.com)

**04–06 JULY 2017**

**WATERMARK CONFERENCE**  
Ekaterinburg, Russia  
[www.watermark-conference.com](http://www.watermark-conference.com)

**04–07 JULY 2017**

**INTERPOL WORLD 2017**  
Singapore  
[www.interpol-world.com](http://www.interpol-world.com)

**24–25 OCTOBER 2017**

**SECURITY DOCUMENT SUMMIT**  
Beijing, China  
[en.sds-china.com.cn](http://en.sds-china.com.cn)

**16–17 NOVEMBER 2017**

**THE HOLOGRAPHY CONFERENCE**  
Barcelona, Spain  
[www.theholographyconference.com](http://www.theholographyconference.com)