Product & Image Security Newsletter

www.productandimagesecurity.org

No. 79 The Newsletter of Product & Image Security Foundation May/June 2011

Contents

Authentication Power to the People

Heidelberg Seeks European Pilots for its newly developed anti-counterfeit tag

Readers of this journal all appreciate that counterfeiting is a fast growing global problem where the range of counterfeits has extended from clothing, shoes and other novelty branded products, into the field of Cosmetics, Personal Health Care, Pharmaceuticals, Food, Wine & Spirits, Home Appliances, Electronic Equipment and batteries, Toys, Power Tools & Equipment and Automotive Spare Parts and is now creating serious health and safety risks which in some cases are life threatening.

The standard of packaging and labelling of counterfeit products has improved significantly over the last decade. In most cases today, it has become extremely difficult for even professionals to tell the difference between a counterfeit and the genuine article. Counterfeiters even go as far as copying quality assurance labels, government test approval and risk markings, product safety certificates as well as the printed warnings that are often used to inform consumers to watch out for counterfeits!

In an attempt to move authentication into the hands of the consumer Heidelberg has developed the '**1-Tag**' which is a combination of 2D barcode, randomly introduced *Page 3 >>*

A new brand protection label has just been developed by Heidelberg; some would say; the most powerful presence in print today

The Product & Image Security Foundation is the leading International Forum for Manufacturers, Users and Suppliers of Security Labels, Documents, Tags, Materials, Systems and Product & Image Security Technologies

This newsletter is published and produced by Product & Image Security Foundation
81 Houting, Dosthill, Tamworth B77 1PB, United Kingdom. Tel: +44 1827 281143. E:Mail jeremyplimmer@aol.com

Quick codes make loads of sense

Will smart phones be the natural future choice for consumer led authentication?

The use of bar coding as an authentication technology is well established, especially where such codes can be adequately protected from unauthorised reproduction.

Packaging and labels can be adapted to carry such coding for track & trace purposes but we all know that there are weaknesses in relying on track & trace in isolation for adequate protection against counterfeit items entering the supply chain.

In some markets it's seen as more effective to protect the product rather than the packaging and herein lies the problem for bar coding suppliers. They often have effective methods of delivering bar codes in linear or 2D format to FMCG products or directly on to components such as car and aeronautical parts but can be frustrated by tiny items such as electronic parts and those goods that need to carry unobtrusive authentication devices such as jewellery, watches and collectable ceramics.

Protecting bar codes from unauthorised replication involves the use of encryption and whilst it is recognised that this is still an effective route, the simpler techniques can now be broken open by determined hackers equipped with tools obtained from their peer groups on the internet.

Six Degrees Counterfeit Prevention, LLC., of Los Angeles has very recently introduced a new method of protecting content stored in a data capacitor, such as a bar code or RFID tag from counterfeit attack through the use of the world's first polymorphic non-mathematical encryption technology.

"Developed in Israel, this method of encrypting the content of a data capacitor is achieved through polymorphic encryption. This method changes the code structure every time each piece of code is written. Moreover the code is pervasive and can be used in other capacitors such as RFID too. It has at minimum a one million bit encryption strength, which is more than enough to protect it from attacks well into the future." Eddie Cohen, CEO of Six Degrees told *Product & Image Security* during a recent interview.

"We protect the code, where only the original content is capable of being authenticated from duplication attack, by making each barcode unique to itself with no two generated results ever being the same. Since each barcode can contain all the entire product data [1] this eliminates the need for an in-front database. Time, money and energy are reduced substantially. Vulnerability to the data base is now non-existent since we check the code itself for conformity and don't need to match it with lists of numbers held on a server somewhere. There is also a measure in place to prevent the same encrypted 2D barcode from being authenticated more than once. So if someone duplicated our barcodes, say 100k times, the second scanned barcode will alert the client and the end user of fraud." Eddie continued.

The data carried by each piece of code can be used for internal track and trace purposes too.

Combine this secure encryption technology with a QRC (Quick Response Code) and a camera phone and you even have an authentication system suitable for use by the consumer. No special hardware is required to generate, print or authenticate a product since the code carries the security, not the 'app' which makes the system even more secure since there is no encryption or decryption software resident in the phone.

Software 'apps' for QR code reading already exist for smart phones and the technology is now fairly common on FMCG products as well as press advertisements, although it's mostly for product promotion rather than authentication at present.

Finally there's the matter of encoding and encrypting small or sensitive items such as jewellery, ceramic collectables and the like, to protect against diversion as well as counterfeit attack. The polymorphic encryption can be applied to any hardened material in 2D code format.

It has to be said that such an encryption technology which combines versatility and high security, has significant attributes when it comes to product protection, since it addresses the authentication needs of brand owners at item level in fields as diverse as pharmaceutical tablets through to microchips. Because the technology is 'seamless' it can be utilised across all segments of the market at pack and pallet level too.

eddie@6dcp.com
www.6dcp.com

[1] *In this form it's termed a micro database-less capacitor—ED*

Additional points in favour of this method of approach:

- Stolen goods such as pharmaceuticals can easily be blacklisted
- Grey market goods are easily detectable if the code is structured correctly
- The expiration date can be covertly embedded within the code thus making any changes identifiable
- The manufacturer can also use the code to collect useful information about the customer at no extra cost
- The code can be used to protect other vulnerable security print items such as lottery tickets, ID's and financial instruments
- The code is e-Pedigree ready as a secure track & trace and authentication system for future legislation in this field