Product Datasheet

NanoDigital^{TM} Ink Technology

V1.0

August 2020

Table of Contents

1 NanoDigital^{TM} Ink

NanoDigital^{TM} is a new security ink that is digital-ready and available as an additive to packaging inks.

The security pigments are based on patented timecoded upconversion nanoparticle (UNCP) technology and are digital-ready with stable dispersion and pigments size < 100nm. Our NanoDigital inks are extremely bright, outperforming standard upconversion pigments which are in the micrometer range.

1.1 Common Security Features

Today physical features used such as holograms, taggants, fluorescent fibers, optically variable inks, anti-scan patterns, guilloche and tactile features, are analog. They are analog because they do not carry digital information and they are not machine readable to a unique identity. These features are commonly used for document and identity security to thwart potential counterfeiting attempts.

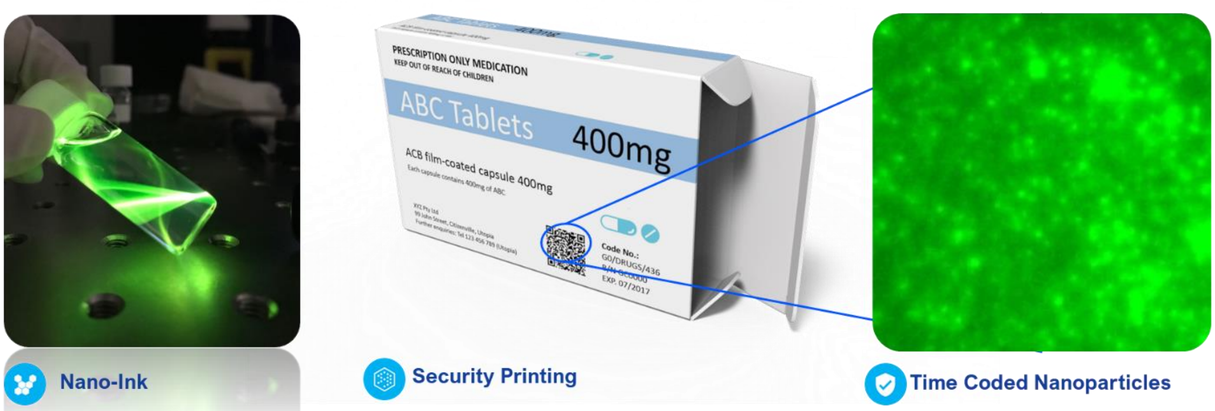
Upconversion security pigments offered to the security printing industry are typically of non-digital because their nanocrystals are of low quality, in the micron-sized range and not dispersible in inkjet inks: They are not digital-ready.

1 Image Source: https://discover.passportindex.org/security/what-secrets-is-your-passport-hiding/, https://regulaforensics.com/en/support/glossary-banknotes/#g640

1.2 Physical Security

NanoDigital^{TM} combines nanomaterials and photonics (nanophotonics). At the nano-level NanoDigital^{TM} utilizes patented technology[1]. The nano-tech enables realization of physical security by engineering of time coded nanoparticles. The nanoparticles have a codable core, which means they emit light when prompted by the reader and are programmed using colour and timecodes. Timecodes are a world-first, giving these nanoparticles an ID. Combining this with digital printing of 2D code provides an unbreakable physical-to-digital link for products.

The NanoDigital^{TM} ink reacts when a reader device probes them with an invisible laser. The inks become excited by the light, and glow. When the laser is switched off the glow starts to decay. It is this feature which is timecoded.


PRESCRIPTION ONLY MEDICATION
KEEP OUT OF REACH OF CHILDREN
ABC Tablets
400mg
ACB film-coated capsule 400mg
Code No.:
EXP. 07/2017

Nano-Ink

Upconversion nanoparticles with high brightness are formulated into advanced transparent digital or packaging inks. The high stability of our upconversion nano-inks enable digitally printable variable data code patterns.

Security Printing

NanoDigital Ink can be applied onto packaging either non-digitally into graphics & branding or into digitally printed barcodes. Security can be extended to the digital domain using our nanoQR and NanoDM technology which uses digitally signed codes. The digital security add on can easily identify product tampering such as expiry date or batch number modification.

Time Coded Nanoparticles

Time-coding is about engineering the way in which nanoparticles glow in response to read light. This glow time provides a dimension for creating inks with complex engineered "DNA". Such advanced security labelling technologies may enable fast identification of physically counterfeit labelling and packaging.

[1] https://patentscope.wipo.int/search/en/detail.jsf?docId=AU231340282 , https://patentscope.wipo.int/search/en/detail.jsf?docId=AU231340281

1.3 Product Offerings

NanoDigital inks are usually supplied as a UV curable formula but can be offered or integrated, as necessary. We offer

- NanoDigital^{TM}: Covert UV curable IR-to-IR (NanoDigital UCNP-804) and IR-to-VIS NanoDigital UCNP-545 for printing covert variable data barcodes. These codes are readable and authenticatable by our dedicated reader device.
- NanoDigital UCNP-804-B: This "B" variant includes black pigmented ink with addition IR-to-IR pigments. This ink is used to print variable data barcodes. These barcodes are readable by the public with their smartphone and authenticatable by authorities using a dedicated reader.
- NanoScreen^{TM}: Heat curable white pigmented PAD and Screen ink with IR-to-IR (NanoScreen UNCP-804-W) and IR-to-VIS (NanoScreen UNCP-545-W). These inks can be used for direct-to-product applications
- NanoPack^{TM}: are for packaging inks, and are supplied as NanoDigital pigment concentrate for Gravure and offset inks

Codes can be printed as standard barcodes or with addition digital security capabilities using our NanoQR^{TM} or NanoDM^{TM} technology.

1.4 Digital-Ready Ink for Securing Variable Data

NanoDigital utilizes the nanotechnology for physical security and can extends to the digital world with any 2D code technology.

NanoQR^{TM} 	QR-code
• Covert (invisible) or visible if printed using pigmented NanoDigital Ink	• Overt (visible)
• Used for authentication, serialization, and tracing	• Used marketing, payments, product coding.
• “3D” code with public open source encoding and decoding, but an additional timecoded security feature of the NanoDigital ink	• 2D code only (binary) with public open source encoding and decoding.
• Protected against duplication by addition of NanoDigital ink	• Not protected against digital or physical copying.
• Secured digitally if you select to use our digital add-on. This uses best practice digital signature standards to bind product data into the code.	• Supports encryption of data prior to storage (but not commonly used)
• Readable using handheld scanners for reading and physical authentication OR by smartphone for reading and digital authentication	• Readable by anyone with a smartphone

Comparison of NanoDigital technology with other digital identification systems

2 Reader Device

HWR-1200 is designed for a highly mobile worker. The device enables authentication of NanoDigital Inks or NanoQR codes and data capture of common 2D Codes. The device is compact and robust integrates with existing data capture workflows. The device pairs with Apple® iOS, Android™, and Windows Mobile® and other devices over WiFi.

HWR-1200 enables workers to accomplish their authentication and data collection tasks with efficiency and agility. HWR-1200 has a high performance 2D imager and proprietary optical module for authenticating the timecoded security feature of NanoDigital inks and codes.

高铭科维
Hand Scanner

3 Digital Security with NanoQR^{TM}

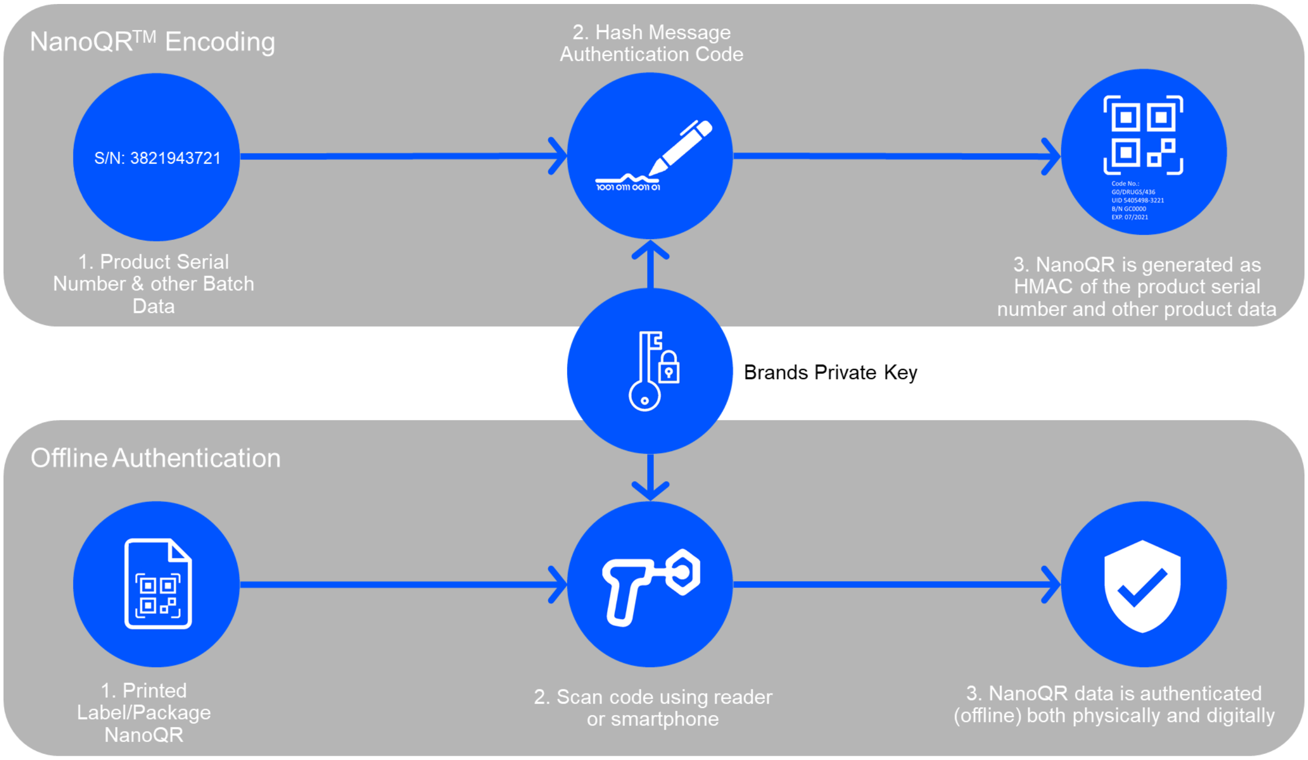
NanoQR^{TM} enables a digital bridge to link the physical product/label and the information security of any data generated or associated with label or product. For example

- Tamper evidence of QR-Codes and information on the same label/product.
- "Proof-of-Scan" protocol which uses a challenge-response between a NanoQR^{TM} on the label and the track-and-trace server, enables a provable audit trail for track and trace information.

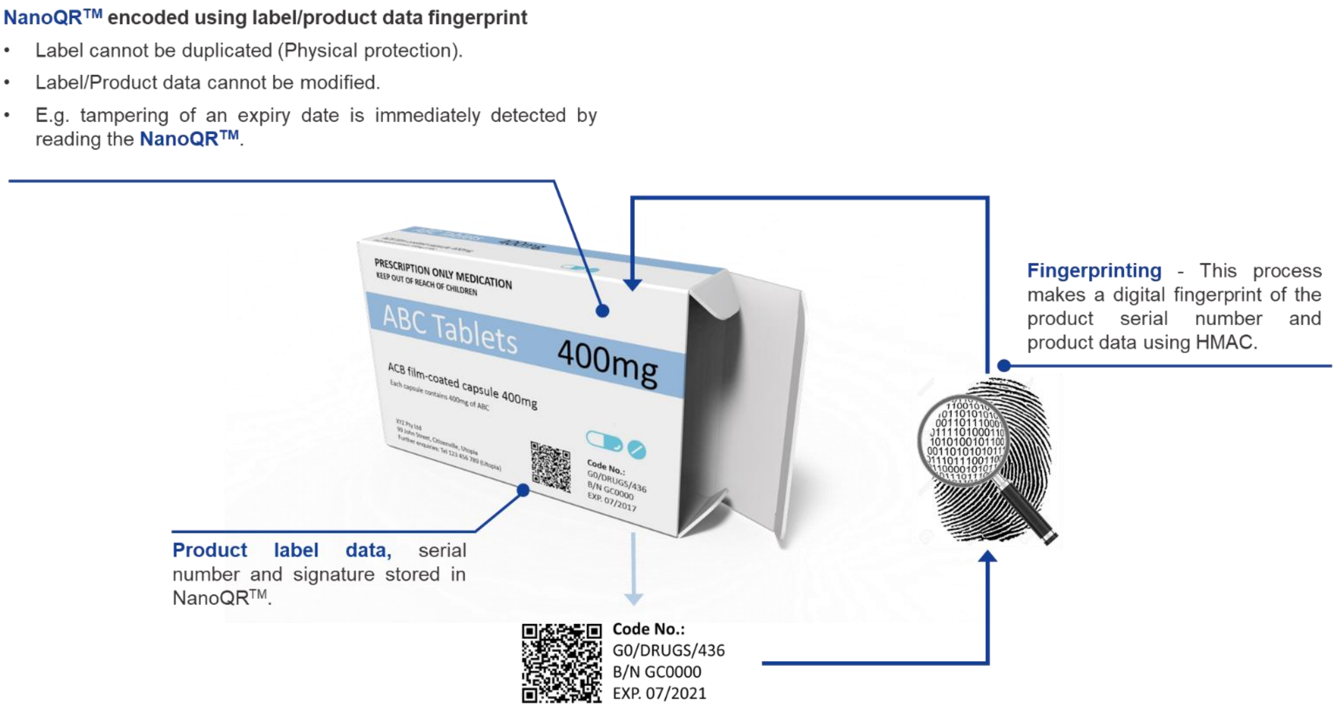
3.1.1 Offline Digital Authentication

A strong method of information security using NanoQR^{TM}, is to generate the NanoQR^{TM} data from a fingerprint of the product serial number and/or other product information. In this way, the NanoQR^{TM} is explicitly "binded" to other information through cryptography. By having the NanoQR^{TM} data generated from a hashed-message-authentication-code (HMAC), the NanoQR^{TM} cryptographically connects

1. Authorities identity
2. Product serial number
3. Other product data


NanoQR™ Encoding
2. Hash Message Authentication Code
S/N: 3821943721
1001 0111 0011 01
Code No.:
G0/DRUGS/436
UID 5405498-3221
B/N GC0000
EXP. 07/2021
1. Product Serial Number & other Batch Data
3. NanoQR is generated as HMAC of the product serial number and other product data
Brands Private Key
Offline Authentication
1. Printed Label/Package NanoQR
2. Scan code using reader or smartphone
3. NanoQR data is authenticated (offline) both physically and digitally

The concept is shown in the diagrams above. The serial number and other product data such as the example of medicine expiry date along with the issuing authorities identify key can be hashed together using HMAC technology and stored in the NanoQR^{TM}. This enables offline authentication where the scanning the NanoQR^{TM} proves that the product data has not been modified. For example, if the NanoQR^{TM} was modified to change the expiry date of the medication, it would no longer match the authentication code encoded into the NanoQR^{TM}.



NanoQR^{TM} encoded using label/product data fingerprint

- Label cannot be duplicated (Physical protection).
- Label/Product data cannot be modified.
- E.g. tampering of an expiry date is immediately detected by reading the **NanoQR^{TM}**.

Fingerprinting - This process makes a digital fingerprint of the product serial number and product data using HMAC.

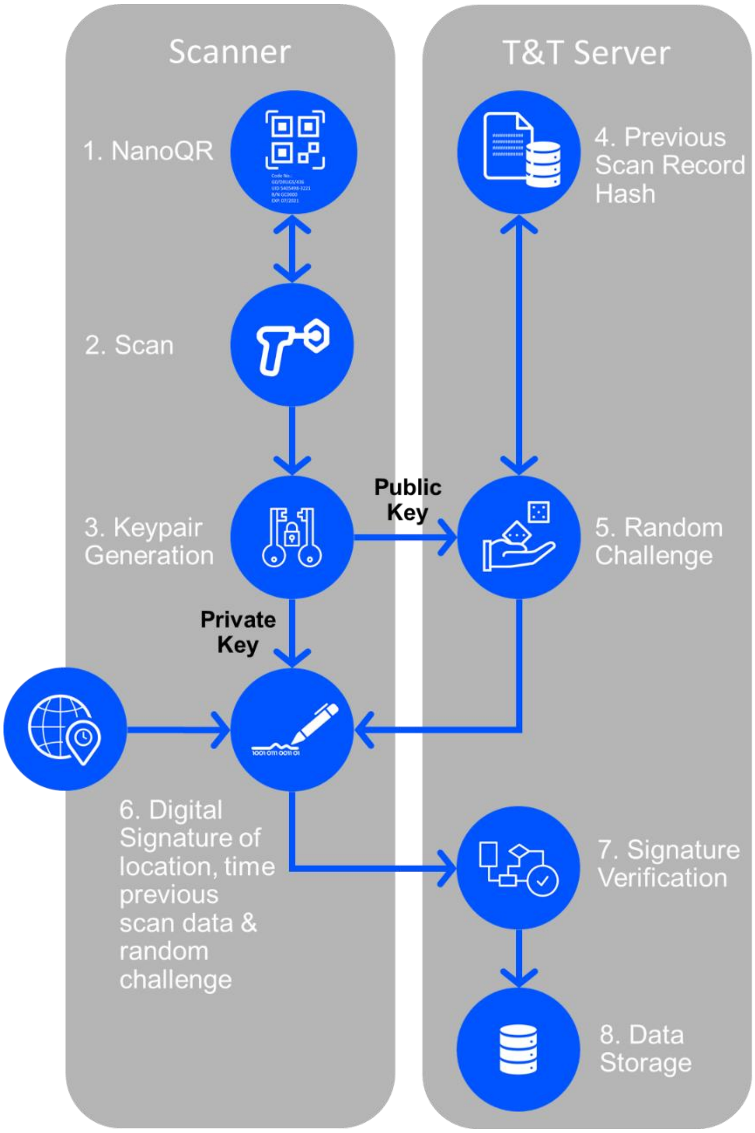
Product label data, serial number and signature stored in NanoQR^{TM}.

3.2 Proof-of-Scan Authenticated Traceability Data

Typical track-and-trace operations involve scanning a barcode and sending location, time and other "scan data" to a server for storage. Many information security breaches are possible with such systems, for example

1. Spoofing: Scanning a photocopy or picture of an original barcode, therefor faking the presence of the label at a scan location.
2. Unauthorised Data Injection: barcode scanners can be simulated by computer software and used to inject false scan records into the track and trace server
3. Data Tampering: authorised or unauthorised persons who have access to the track-and-trace server can modify records.

NanoQR^{TM} enables a patented "proof-of-scan" mechanism which is shown in the diagram below. This technology is a form of challenge-response protocol between a track-and-trace server, the scanner and each package/label.


Scanner
T&T Server
1. NanoQR
4. Previous Scan Record Hash
2. Scan
Public Key
3. Keypair Generation
5. Random Challenge
Private Key
6. Digital Signature of location, time previous scan data & random challenge
7. Signature Verification
8. Data Storage

Essentially the “proof-of-scan” provides strong audit evidence that the real original label/package was scanned at a location. This enables authenticated traceability because only the original label/package with specific NanoQR^{TM} can provide the track-and-trace server with a valid digital signature. This is because the valid digital signature can only be generated by combination of the three sources of information: the NanoQR^{TM}, the scanner and the challenge/previous scan data from the server.

In detail, the steps shown in the diagram on the previous page are

❶ NanoQR^{TM} is printed directly on the label or product packaging, and cannot be separated. It is only authenticatable using our reader system which verifies that time-code of the NanoQR security ink. This essentially ensures that “spoofing” attacks are improbable.
❷ Only the interaction between each NanoQR^{TM} and scanner generates a valid private-public keypair based on PKI.
❸ The public key acts as the unique identifier (UID) for the label/package and is sent to the track-and-trace server.

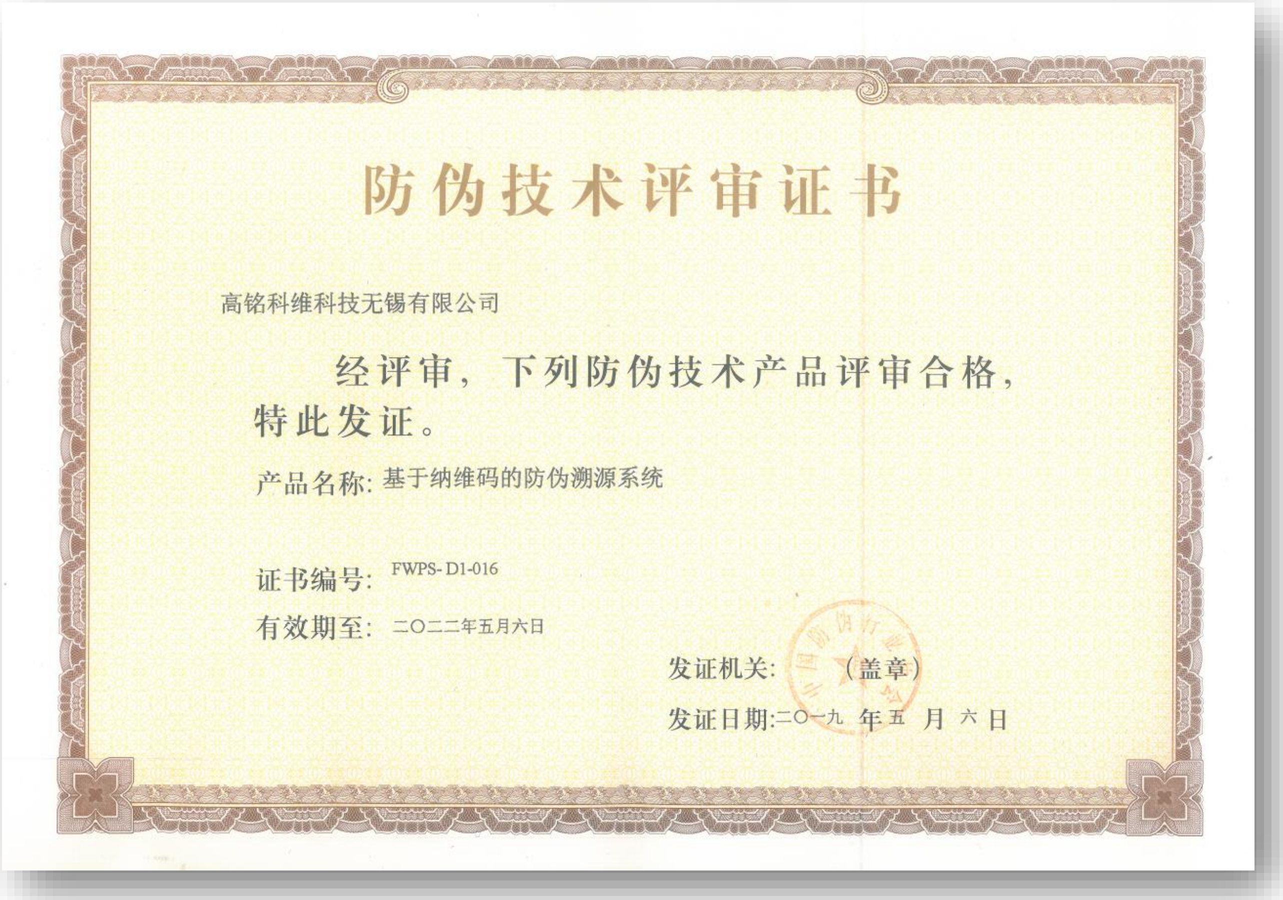
❹ The server responds by retrieving some previous scan information for the purpose of establishing a timestamp of the true order of scan records within its database.
❺ The server combines a hash of the previous scan record with a randomly generated number called a “challenge” and sends this to the scanner.
❻ The scanner takes the received information and combines it with other relevant data such as location and time, then digitally signs this data with the private key, which unique to the interaction of the scanner and NanoQR^{TM} (from step ❷), and then sends it to the server.
❼ The server verifies the data received from the scanner ensuring that the data belongs to the NanoQR^{TM} (public key) and the public key is registered to the correct authority. The purpose of the “challenge” from step ❺ is to prevent “replay attacks”.

This type of scheme cannot be achieved with a standard 2D Barcode based track-and-trace system because the remote scanner may be scanning a physical copy of a label, or a photo of a label. At best, only the scanning device can be authenticated, but not the label/package.

While the use of digital signatures and challenge-response algorithms are not new, the revolutionary step using NanoQR^{TM} is that it provides this link all the way to the original physical label/package. In addition, even admins of the track-and-trace server cannot modify or tamper scan records because the digital signatures originate from the interaction between the scanner and the NanoQR^{TM} on the label/package. Modifying data will be highly tamper evident because the digital signature will not match and fraudulently modified data.

4 Certification

NanoDigital^{TM} is certified for sale in China by the CTAAC (China Trade Association for Anti-Counterfeiting).



防伪技术评审证书

高铭科维科技无锡有限公司

经评审，下列防伪技术产品评审合格，特此发证。

产品名称：基于纳维码的防伪溯源系统

证书编号：FWPS-D1-016

有效期至：二〇二二年五月六日

发证机关：（盖章）

中国防伪行业协会

发证日期：二〇一九 年五 月 六 日

The official anti-counterfeit organization CTAAC (China Trade Association for Anti-Counterfeiting) was established in 1995 by the government’s China Quality Supervisory Bureau. It is responsible for both establishing anti-counterfeiting plans and regulations and monitoring the marketplace for counterfeit goods.

5 Technical Specifications

The following technical specification is an example of a NanoDigital Ink.

NANODIGITAL INK

1 PRODUCT DESCRIPTION

NanoDigital: Covert UV curable IR-to-IR (NanoDigital UCNP-804) and IR-to-VIS NanoDigital UCNP-545 for printing covert variable data barcodes. These codes are readable and authenticatable by our dedicated reader device. NanoDigital UCNP-804-B: This “B” variant includes black pigmented ink with addition IR-to-IR pigments. This ink is used to print variable data barcodes.

UV curable ink suitable for a wide variety of plastic substrates.

2 SUBSTRATES

PMMA/ acrylic glass, Polycarbonate (PC), polyvinyl chloride (PVC), and many more

3 FEATURES & BENEFITS

Fast cure under UV irradiation. Superior chemical and abrasion resistance.

4 SPECIFICATIONS

Supply Format	In 200mL amber glass container.
Colour	Clear slightly yellow; Green under IR radiation
Viscosity	41 ± 1 cp @ 25 °C
Flashpoint	150 ± 30 °C
Storage temperature	18-25 °C
Application temperature	37-42 °C for printing
Shelf life	6 months

5 APPLICATION

Low VOC, low migration UV inkjet for general purpose. Not suitable for food packaging or medical devices

6 SURFACE PREPARATION

Ensure surface is clean, dust and grease free.

If detergent or solvents are used for cleaning, ensure surface is completely dried prior to printing.

7 APPLICATION METHOD

Inkjet printing

8 CURING

Using mercury lamp (medium pressure), 75-200mW/cm^2. 120W/cm width for continuous printing operation. ink cures generally less than 1 second.

UV LED curable on some substrates, such as PVC, minimum power 2W/cm^2 , wavelength 395 nm, 1-2 seconds.

For any new substrate, tests need to be done to achieve best performance.

9 STORAGE INSTRUCTIONS

Store in cool and dry environment. Strictly avoid direct light exposure.

10 PACKAGING

Amber glass container, 200 mL capacity.

11 PRECAUTIONS

Once opened, use withing 3 months.

Avoid contamination of dust or chemicals such as water, ethanol or IPA. A small amount of chemical can cause pigment precipitation which may cause nozzle failure.

Shake well before use. Make sure no bubble in the ink when install. Once installed, ink is stable for 5 days.

12 REGULATORY COMPLIANCE

. Please follow local regulations relating to safety use and dispose of the product.

13 Frequently Asked Questions

What is NanoDigital^{TM}?

- NanoDigital is new security ink combining nanotechnology, photonics and secured digital technology.

How is NanoDigital^{TM} applied?

- It is applied directly to the substrate using inkjet systems, or used in other packaging ink systems.

What are the physical security features of NanoDigital^{TM}?

- NanoDigital^{TM} is a covert technology which is optically activated and readable by NIR illumination
- It has strong physical security by means of patented timecoded nanocrystal pigmented ink ("nanoink")
- It can be physically authenticated by luminescence lifetime property (glowing properties)
- It can be physically authenticated by spatial-spectral arrangement (emission spectrum properties)

What are the Digital Security Features of NanoDigital^{TM}?

- NanoDigital^{TM} combine with a 2D Code stores an encrypted Unique Identity (UID) for each label
- NanoDigital^{TM} can be binded with external data and an issuing authority using digital signature technology

How is NanoDigital^{TM} Authenticated?

- NanoDigital^{TM} is readable with a proprietary scanner.
- In standard situation this operates similarly to a barcode scanner

INPI ASIA PTE LTD

101 Cecil Street, #11-04, Tong Eng Building, Singapore 069533
TEL: +65 85 155 637

E: info@inpiasia.com