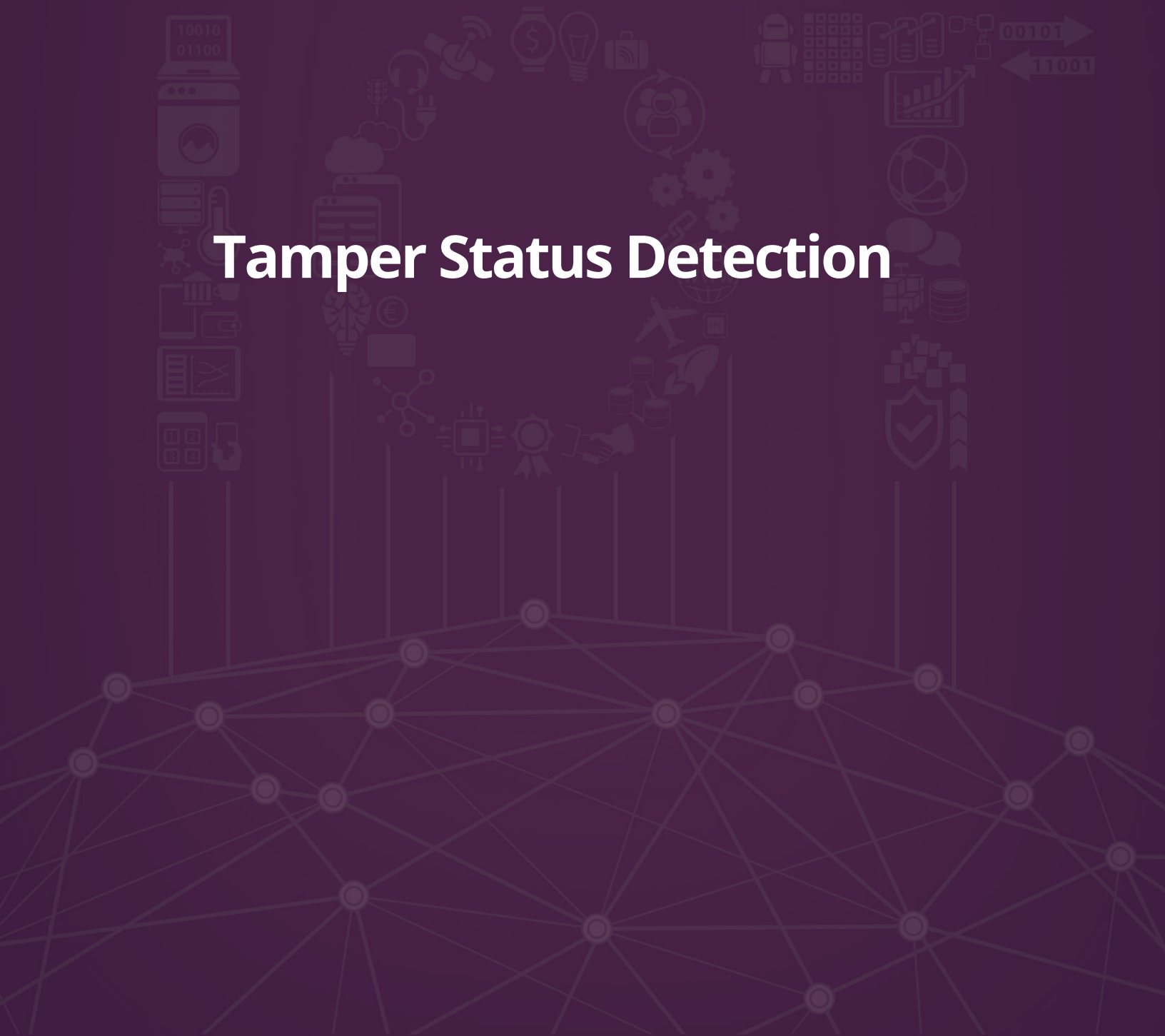
IDENTIV USE CASE



Tamper Status Detection

Problem

Tamper detection is the ability of a device to sense through interrogation by a near field communication (NFC) reader that an active attempt to compromise its integrity, or the data associated with that device, is in progress. The immediate detection of the threat may enable the device to initiate appropriate and swift defensive actions.

Medical devices, utility meters, and many other types of enclosed electronic systems need a robust way to sense unauthorized tampering and to protect the system and its data if tampering occurs.

In medical devices, impaired performance resulting from a tampering event could cause serious harm to patients. Tampering in meters could be a deceitful act leading to a loss of revenue for the utility company. A secure, permanent means of detecting tampering in devices is of critical importance.

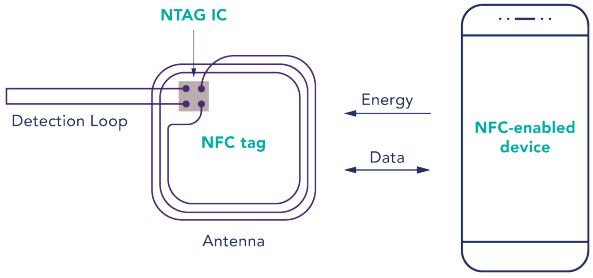
Challenges in Tamper Status Detection

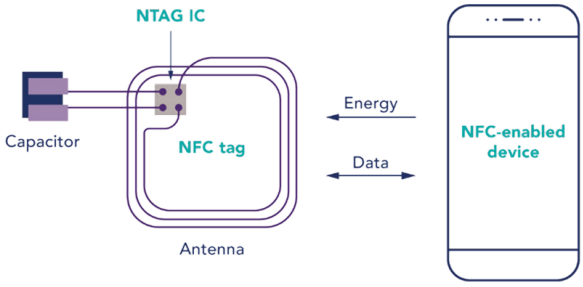
The tamper-evident labels market is estimated at $14,329 million in 2022 and is projected to reach $24,244 million by 2032, at a CAGR of 5.4% from 2022 to 2032.

Today's packaging companies are focused on incorporating tamper-evident properties into products to enhance their functionality and safety, and to comply with strict regulations. According to Grand View Research, under the Commission Delegated Regulation (EU) 2016/161, drug makers are required to add a unique identifier and an anti-tampering device to the packaging of most centrally authorized pharmaceutical products.

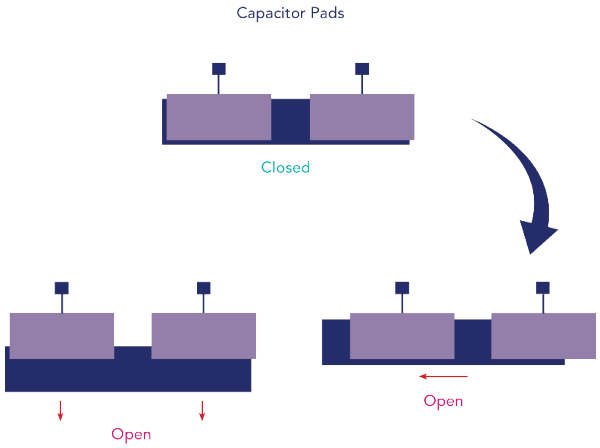
Our Solution: Identiv's Conductive and Capacitive Tamper Status Detection Tags with NXP's NTAG® 22x DNA StatusDetect Chip Line

NXP's NTAG 22x DNA StatusDetect is an innovative, single-chip solution offering cryptographic security, innovative tamper detection, and battery-free sensing. The technology uses multi-layered protection to support a broad range of NFC-based applications that can be trusted to protect products, services, and Internet of Things (IoT)-driven user experiences at scale.





NTAG 22x DNA tags are NFC Forum Type 2 tags and are Common Criteria EAL 3+ certified. There is flexibility to select between two modes to detect tampering: conductive or capacitive tamper detection. There is no need for a dedicated app.



Benefits of Conductive and Capacitive Tamper Status Detection Solution

The NTAG 22x DNA StatusDetect IC comes with SUN (Secure Unique NFC) message authentication. The IC can automatically add its UID, incremental tap counter, and the status to the programmed NDEF (NFC Data Exchange Format) message through ASCII mirroring, and uses an AES-128 key to secure the message with a CMAC (cryptographic message authentication code). The SUN functionality supports advanced protection to verify tag and message authenticity and integrity while enabling secured unique user experiences served in real-time.

NFC Interface

- **NFC Forum Type 2 Tag and ISO/IEC 14443-A compliant**
- **Common Criteria AEL3+ (AVA_VAN.2) certified**
- **7-byte UID**
- **50pF input capacitance**
- **Communication baud rate at 106 kbps**

Memory

- **User memory of 144 (NTAG 223 DNA StatusDetect) or 208 bytes (NTAG 224 DNA StatusDetect)**
- **Ten-year data retention**
- **100 k write cycles**

Security

- **Customizable originality signature (48-byte based on ECC)**
- **SUN message authentication code protected with AES-128**
- **Memory protected with 32-bit password (NTAG 223 DNA StatusDetect) or with mutual authentication with AES-128 bit key (NTAG 224 DNA StatusDetect)**

Status Detection

- **Conductive or capacitive tamper status detection**
- **Capacitive sensing interface to measure environmental conditions**
- **Measurement range is up to 11pF with a resolution of up to 64 steps**

Conductive vs. Capacitive Status Detection

Conductive (resistive) tamper detection uses a loop connected to the IC. A quick readout with an NFC phone verifies if the loop is still intact. If it is broken, the once-opened status is irreversibly stored in the IC memory and reported to the cloud as part of the SUN authentication message, all with a simple NFC phone tap.

For capacitive tamper detection, the IC needs to be connected to a sensing capacitor. When read with an NFC phone, the IC measures the capacitance parameters, and when these exceed pre-configured limits, it provides the open status information. These tags must be calibrated at the customer's production site. The precise position of the capacitor electrodes is difficult to duplicate if manipulated, even a small displacement will result in a different detectable capacitance value when interrogated.

When to Use Conductive vs. Capacitive Tags

Conductive tamper detection is well suited to labels and seals attached to product packaging. The capacitance tag tamper feature enables an easier integration into special form factors, such as a bottle closure, and is also harder to be reconstructed by fraudsters

Before the NTAG 22x chip family, conductive tamper functionality was the only technology available. Now conductive *and* capacitive tamper functionalities are available. Capacitive fill level sensing technology is also an option.

Top Use Cases

Open/close detection is most commonly used in:

- **Wine and spirits**
- **Cosmetics**
- **Pharmaceutical products and medical devices**
- **Smart packaging**
- **Security sealing**

It can also detect if a meter, thermostat, or e-lock was opened, while tamper evidence could be used for warranty voidance or further investigation.

Tamper status detection tags could additionally be used to boost consumer experiences with status-aware content. With an antenna and loop added to a box, a customer could break the loop to opt into a contest. Kraft Heinz used Identiv's NFC-enabled tag and NXP's NFC NTAG connected solution to create the 2019 IoT Integration Award-winning "Find the KRAFT Golden Singles" reward scratch game. The NFC-enabled tags were embedded into KRAFT Singles 24-count instant redeemable coupon (IRC) labels, which were available at Walmart.

Find out more about Identiv's RFID, NFC, and inlay portfolio:

Call +1 888.809.8888
Email transponder_sales@identiv.com
Visit identiv.com