IDENTIV USE CASE

Advanced IoT Security

Problem

The growing constellation of connected Internet of Things (IoT) devices is transforming how we collect, exchange, analyze, and extrapolate huge amounts of data. Companies gather insights into everything, from understanding user behavior to increasing business efficiencies. As connected IoT devices continue to increase in number, it is more challenging for businesses to secure them and keep threats at bay. In the consumer product space, brands need to ensure their digitized products are connected and their identities are verified.

Challenges Associated with IoT Security

According to Organisation for Economic Co-operation and Development (OECD) data on counterfeiting and international trade, the total value of counterfeit and pirated goods was about $1 trillion in 2013 and is expected to grow to close to $3 trillion in 2022.

IoT devices are attractive targets for cybercriminals because they offer an attack surface ripe for security breaches. Whether companies are beginning to adopt IoT or looking to expand their established IoT networks, all experience similar challenges when it comes to managing, monitoring, and securing their connected IoT environments.

To secure a connected IoT ecosystem, only a complete solution can prevent bad actors from hunting for and exploiting gaps from many more attack surfaces. You need support for:

- **Item-level authentication**
- **Open status detection against tampering and refill fraud**
- **Protection of sensor/sensing data against manipulation**

Our Solution: NFC Tags with NXP NTAG 22x Chip Series

With near field communication (NFC), products are smarter, more interactive, and more traceable — they can talk to each other and to smart devices — making the IoT more trustworthy.

Based on the Advanced Encryption Standard (AES), Identiv's NFC Tags with the NXP® NTAG® 22x chip series use symmetric key encryption, meaning there is only one secret key and the same key is used for encryption and decryption. The tags provide capabilities for advanced anti-counterfeiting, innovative tamper detection, or batteryless condition sensing.

Identiv's NFC-enabled solutions verify identities and security in the IoT and are embedded in billions of everyday objects, including medical devices, books, toys, apparel, perishables, and pharmaceuticals. Our NFC app development, MedTech and pharma, authentication, anti-counterfeiting and brand protection, sensing, and UHF solutions let you create your own products, ecosystems, and experiences.

Benefits of Identiv NFC Tags with NXP NTAG 22x Chips

- **Can be conveniently applied in/on products**
- **Offer an invisible security solution**
- **Cannot be removed easily; re-using is practically impossible**
- **Encryption adds another layer of security to the solution**
- **Battery-less sensing means more cost-efficient, sustainable solutions**
- **SUN and tamper status readout without an app; for sensing, you need a mobile or web application to interpret measurement data**
- **Extremely end-user friendly solution**
- **Can be used in a range of fields, including valuable commodities, luxury goods, industrial supply chains, and more**

Top Use Cases

1. Cryptosecurity

NFC tags can be used to provide cryptosecurity, meaning cryptographic keys are used on both sides of the communication. When data is protected through cryptographic means, the NFC system is better protected against data fraud or manipulation.

Cryptographic algorithms and keys can be symmetric or asymmetric. By using cryptography to achieve information security goals, you can guarantee the data cannot be read or changed by an unauthorized entity.

Crypto-secure Identiv NFC Tags with the NXP NTAG 22x chip series and a symmetric cypher can be used to support product authentication and integrity, while enabling status-aware messaging. This helps prove brand authenticity and provide a trusted, secure method of customer interaction with products like high-value retail items.

2. Anti-Counterfeiting

Counterfeit items are a worldwide challenge across all industries. They can result in lost sales, damaged brand reputation, liability bills, and poor customer experiences. Embedding NFC security tags into goods authenticates the products and improves the user's experience, increases customer loyalty, and enhances product functionality.

For improved customer interaction, Identiv NFC Tags with the NXP NTAG 22x chip series enable product authentication using NFC smartphones and other smart devices. The tags' ICs can go beyond identification (with a unique international identifier or UID) to provide a secure dynamic authentication mechanism.

A capacitive or conductive tamper design will, upon manipulation, result in an irreversible once-opened status when read with an NFC device. The tags are self-destructive and are destroyed upon removal. The once-opened message is sent to the cloud for detection.

Tamper-proof NFC tags can be applied to items such as luxury goods, spirits, home appliances, and medicines, and are mounted using a permanent, high-performance self-adhesive. The tags relay information to the end-user, like promotional material or product information, enhancing personal 1:1 consumer engagement.

Any brand utilizing these specific tags will be the single, exclusive owner of those tags' numbers. Users can very easily authenticate a product and confirm it is not a fake. The NFC tag acts as an electronic certificate of authenticity. These tags can tell you if, for instance, a product is genuine or if a piece of safety equipment is original. As a result, you can quickly identify any counterfeit items.

The NFC (NDEF) message read from DNA tags has added security attributes that dynamically change on every NFC phone tap, which means the taps cannot be cloned. Each time a tag IC is tapped, it generates a Secure Unique NFC (SUN) authentication message using an AES-128 cryptogram.

Beyond SUN authentication, the tags allow mutual authentication, meaning only authorized devices (with the right key) can access protected user memory.

These custom-designed NFC tags can be embedded into products (e.g., luxury goods, wine and spirits, etc.) or applied to products (e.g., package seals and drug delivery devices). The tags can then be read by a device to ensure user safety and proper configuration.

3. Supply Chain Fraud

The SolarWinds cyber incident revealed supply chain vulnerabilities can compromise entire systems. Many existing state-of-the-art supply chain protocols depend on centralized processing, including the coinciding weaknesses hackers leveraged in the SolarWinds attack.

Using Identiv NFC Tags with the NXP NTAG 22x chip series to detect fraud brings unprecedented security and efficiency to supply chain management. These tags can be used to prevent three types of fraud in the supply chain, including:

- **Modification of product details, such as quality inspection date, if protected with mutual authentication (i.e., protected memory content)**
- **Cloning genuine product details onto a counterfeit product's tag by checking tag originality in combination with SUN online authentication**
- **Protection against any message replay attack where transmitted data is fraudulently repeated with SUN message protection**
- **Reapplication of a tag from a genuine product and attaching it to a counterfeit if the tag's tamper structure is destroyed and/or opening status is captured**

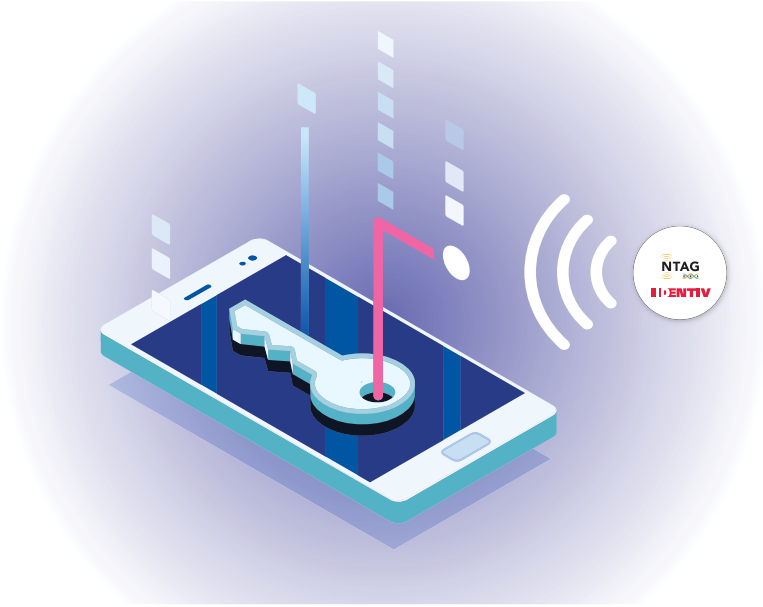
Centralized supply chain systems suffer from these three frauds because of a lack of transparency. These NFC tags can help you safeguard the supply chain with improved tracking, traceability, and control.

4. Tag, Message, and Mutual Authentication

Tag and Message Authentication: Using AES-128 encryption, the feature by NXP automatically generates a unique secure authentication code each time the tag is tapped. This allows unique communication to each user based on predefined criteria and is based on the verification of a genuine tag and message in the backend (e.g., the cloud).

Only an NFC-enabled smartphone is required to have the tag generate this tap-unique data consisting of CMACed information derived from the chip UID, a tap counter, and status value, making taps unclonable.

Mutual Authentication: An app is required for mutual authentication. The tag and reader identify each other using the same key, preventing unauthorized access. These tags use the AES-three-pass mutual authentication protocol utilizing a UID-diversified AES authentication key.



Want to learn more about Identiv's NFC tags?

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