Proof of Presence: A Secure Authentication and Verification Mechanism for NFC-enabled Devices with Tokenization, NFTs, and Digital Product Passport

Abstract

The **Proof of Presence** mechanism offers a secure, robust, and verifiable method to authenticate the presence and ownership of physical objects via NFC-enabled devices. Leveraging NXP's **NTAG 424 DNA TT** technology, this system integrates **AES-128 encryption**, **Cipher-based Message Authentication Code (CMAC)**, **Secure Unique NFC (SUN)**, **tokenization**, **Non-Fungible Tokens (NFTs)**, and the **Digital Product Passport (DPP)** standard. This paper details the processes involved in writing, reading, and verifying data using these cryptographic measures. By adding tokenization and NFTs, the Proof of Presence concept also extends into the realm of digital ownership and traceability. These components collectively form a secure, interoperable solution for anti-counterfeiting, tamper detection, and product verification in supply chains, circular economy systems, and beyond.

---

1. Introduction

As the demand for digital verification of physical products grows, technologies like NFC (Near Field Communication) have gained widespread adoption. However, the simplicity and convenience of NFC create vulnerabilities such as counterfeiting and tampering. To mitigate these risks, NXP's **NTAG 424 DNA TT** enables cryptographic security with **AES-128**, **CMAC**, and **SUN** for enhanced authentication and verification.

In addition to the traditional cryptographic measures, **tokenization** and **Non-Fungible Tokens (NFTs)** are emerging as powerful tools in creating immutable digital identities for physical objects. Furthermore, the **Digital Product Passport (DPP)** standard is becoming central in promoting product transparency and traceability, essential in industries such as manufacturing, luxury goods, and the circular economy. This whitepaper outlines the process of Proof of Presence and its integration with tokenization, NFTs, and the Digital Product Passport standard.

---

2. Proof of Presence: Overview of Core Mechanisms

The **Proof of Presence** mechanism consists of several key processes:

- **Encryption and Cryptographic Messaging**: Ensuring the integrity and confidentiality of data during communication between the NFC tag and the reader device.

- **Tokenization and NFTs**: Attaching a digital identity to each physical product, creating a link between the physical and digital realms.
- **Digital Product Passport (DPP)**: Providing a standardized and interoperable way to store and share product information.

These mechanisms form a complete solution for secure authentication and verification of physical products using NFC.

---

3. Cryptographic Techniques for Proof of Presence

3.1 AES-128 Encryption

The NTAG 424 DNA TT uses **AES-128** (Advanced Encryption Standard with a 128-bit key) to secure data during transmission. AES-128 is a symmetric encryption algorithm widely used for its balance of security and efficiency. For Proof of Presence, AES-128 ensures the confidentiality of product metadata, sensitive data, and any tokenized information stored on the NFC tag.

- **Session Keys**: During an interaction (either read or write), the NFC reader and tag generate session keys (`SesAuthENCKey` and `SesAuthMACKey`). These keys are derived using random challenges (`RndA` and `RndB`) exchanged during the authentication process.
- **Encryption Flow**: Data is encrypted using `SesAuthENCKey` before being sent from the NFC tag to the reader. This ensures that even if the data is intercepted, it remains confidential.

3.2 CMAC (Cipher-based Message Authentication Code)

CMAC is used to provide data integrity and authenticity. After encrypting the data, a CMAC is calculated using the `SesAuthMACKey`. The CMAC serves as a verification token, ensuring that the data has not been tampered with during transmission.

- **CMAC Flow**: A CMAC is calculated over the data to be sent, combined with the Transaction Identifier (TI) and Command Counter (CmdCtr), ensuring that each message is unique and tamper-proof.
- **Verification**: Upon receiving the data, the NFC reader recalculates the CMAC and compares it with the CMAC received from the tag. If the two match, the data is verified as authentic and intact.

3.3 Secure Unique NFC (SUN)

The **SUN** (Secure Unique NFC) feature generates a unique message for each NFC tap. This dynamic authentication mechanism ensures that each interaction with the tag results in a unique verification code, making replay attacks or cloning ineffective.

- **SUN Flow**: Every time the tag is tapped by an NFC device, a SUN message is generated, containing a unique counter, UID (Unique Identifier), and other authentication data, encrypted using AES-128.
- **Verification**: The SUN message is sent to the host server, which verifies the uniqueness of the interaction and checks the validity of the message.

---

4. Tokenization and Non-Fungible Tokens (NFTs)

4.1 Tokenization Process

In the context of Proof of Presence, **tokenization** refers to the process of assigning a unique, digital identity to a physical product. This is achieved by creating a digital token that represents the product's metadata, ownership information, and lifecycle details.

- **Token Structure**: The token consists of the product's metadata (e.g., product name, ID, manufacture date, expiration date, batch number) and a unique identifier (UID) stored on the NTAG 424 DNA TT.
- **Token Security**: The token is encrypted and linked to the physical product using the secure messaging capabilities of the tag, ensuring that it cannot be duplicated or tampered with.

4.2 Non-Fungible Tokens (NFTs) for Proof of Ownership

Once the token is created, it can be represented as a **Non-Fungible Token (NFT)** on a blockchain. NFTs are unique digital assets that prove ownership of a particular product, and they are immutable and traceable. In this Proof of Presence framework:

- **NFT Creation**: An NFT is generated for each tokenized product and stored on a blockchain. This NFT contains the unique identifier of the product, product metadata, and a link to the product's **Digital Product Passport (DPP)**.
- **Ownership Verification**: When the physical product is tapped by an NFC-enabled device, the Proof of Presence mechanism can verify ownership by checking the linked NFT on the blockchain.
- **Transfer of Ownership**: The NFT allows for easy transfer of ownership of physical products by transferring the associated NFT to a new owner on the blockchain.

---

5. Digital Product Passport (DPP)

5.1 Overview of DPP Standard

The **Digital Product Passport (DPP)** is a standardized digital record that stores essential information about a product, such as its origin, materials, manufacturing details, and lifecycle. The DPP is an essential component of the **circular economy**, enabling companies and consumers to track a product's sustainability, recyclability, and ownership history.

- **DPP Integration with NFC**: Each NTAG 424 DNA TT tag is linked to a product's DPP, ensuring that key product information is accessible by simply tapping the product with an NFC-enabled device.
- **DPP Data Structure**: The DPP includes critical data such as:
  - Product origin and manufacturer
  - Materials and components
  - Usage history and maintenance logs
  - Recycling and disposal instructions
- **Interoperability**: The DPP follows standardized formats such as those proposed by the **European Union** for Digital Product Passports, allowing interoperability across different systems and industries.

5.2 DPP Verification Process

- **Data Access**: When a product is tapped by an NFC device, the DPP can be accessed in real-time. This allows consumers, regulators, or businesses to view essential product data and verify its authenticity.
- **DPP and Circular Economy**: The DPP ensures traceability throughout the product's lifecycle, helping companies adhere to sustainability standards and enabling easier recycling or repurposing of materials.

---

6. Example Scenario: Proof of Presence for a Tokenized Product with DPP and NFT

6.1 Writing Product Metadata to the Tag

A luxury watch manufacturer integrates an NTAG 424 DNA TT tag into its products, linking each watch to its **Digital Product Passport** and creating an associated **NFT** on a blockchain.

- **Product Metadata**:
  1. Product Name: "Omega Speedmaster"
  2. Product ID: "OMEGA12345"
  3. Manufacture Date: "2024-08-15"
  4. Warranty Expiration: "2029-08-15"
  5. Batch Number: "W123"
- **Writing Process**:

1. The product metadata is tokenized and stored on the NFC tag.
2. The tag encrypts the metadata using **AES-128**.
3. A **CMAC** is generated for the metadata to ensure data integrity.
4. The **NFT** representing the product is created on the blockchain and linked to the product’s DPP.

6.2 Reading and Verifying the Product

A potential buyer taps the watch with their NFC-enabled phone, triggering the **Proof of Presence** mechanism.

- **Verification Steps**:
    1. The NFC device authenticates the tag using **AES-128** encryption.
    2. The product metadata is decrypted and verified using the **CMAC**.
    3. The **SUN message** is generated, ensuring the authenticity of the interaction.
    4. The phone retrieves the **Digital Product Passport (DPP)** from a linked server, showing product origin, warranty, and ownership details.
    5. The device verifies the product’s **NFT** on the blockchain, confirming ownership.

---

7. Conclusion

The **Proof of Presence** mechanism provides a comprehensive solution for verifying the authenticity, ownership, and lifecycle of physical products using NFC technology. By integrating **AES-128 encryption**, **CMAC**, **SUN**, **tokenization**, **NFTs**, and the **Digital Product Passport (DPP)** standard, this approach ensures the security and traceability of products in industries such as luxury goods, supply chain, and the circular economy.

The combination of cryptographic security and tokenization through NFTs bridges the gap between the physical and digital worlds, creating new opportunities for product verification, ownership transfer, and lifecycle management.