Claims

1. A system for physical-digital authentication of a good, said system comprising:

a physical component associated with said good, said component exhibiting an intrinsic and stochastic surface micro-geometry such as to constitute a Physical Unclonable Function (PUF);

a Near Field Communication (NFC) chip integrated in said good, said chip comprising a Secure Element;

a Distributed Ledger Technology (DLT) platform;

characterized in that:

a digital fingerprint (PUF fingerprint) is generated by processing data acquired from a surface scan of said intrinsic micro-geometry (PUF) of the component;

said Secure Element is configured to securely store an encrypted digital token, said digital token being representative of at least said PUF fingerprint;

said DLT platform is configured to immutably store a cryptographic hash, said hash being calculated from information contained in said encrypted digital token.

2. The system according to claim 1, wherein said surface scan is a high-resolution three-dimensional scan, such as structured light scanning or confocal laser scanning, suitable for capturing stochastic imperfections of the component surface.

3. The system according to any of the preceding claims, wherein said PUF fingerprint is a binary code generated by a process of processing a three-dimensional point cloud acquired from said scan, said process comprising the steps of:

acquiring said three-dimensional point cloud;

identifying a set of stable and geometrically salient keypoints on said point cloud;
computing a local descriptor for each of said keypoints, said descriptor being representative of the local geometry around the keypoint;
generating a binary code by aggregating and binarizing the set of said local descriptors.

4. The system according to claim 3, wherein:
said keypoints are identified by means of a geometrically salient feature detection algorithm, such as Intrinsic Shape Signatures (ISS);
said local descriptors are computed by means of a local geometric description algorithm, such as Fast Point Feature Histogram (FPFH);
said binarization is performed by means of a Locality-Sensitive Hashing (LSH) algorithm.

5. The system according to any of the preceding claims, wherein said NFC chip is a passive chip and said Secure Element is a tamper-resistant microprocessor certified according to international security standards, such as Common Criteria with Evaluation Assurance Level EAL5+ or higher.

6. The system according to any of the preceding claims, wherein said encrypted digital token is encrypted by means of an authenticated symmetric-key encryption algorithm, and wherein:
a unique encryption key (K_device) for said NFC chip is cryptographically derived by means of a Key Derivation Function (KDF) from a master key (K_master) and a unique identifier (UID) of said NFC chip;

said master key (K_master) is stored exclusively within a Hardware Security Module (HSM).

7. A method for verifying the physical-digital authentication of a good, said method employing a system according to any of claims 1 to 6, said method comprising the following steps:

a) acquiring, by means of a surface scan of the physical component of the good, a PUF fingerprint of the reading (Ft);

b) reading, by means of a reader device, the encrypted digital token stored in the Secure Element of the NFC chip;

c) calculating a current hash on the encrypted digital token read in step (b);

d) retrieving from the DLT platform a reference cryptographic hash associated with the good;

e) performing a first (digital) comparison between said current hash and said reference cryptographic hash;

f) if and only if said first comparison is positive:

(i) transmitting said encrypted digital token to a secure processing entity and, within said entity, decrypting said token to obtain the reference PUF fingerprint (Fm) contained therein;

(ii) performing a second (physical) comparison between the reading PUF fingerprint (Ft) and the reference PUF fingerprint (Fm);

g) confirming the authenticity of the good if and only if both comparisons, the first (e) and the second (f.ii), are positive.

8. The method according to claim 7, wherein said second (physical) comparison in step (f.ii) comprises

calculating a distance metric, such as Hamming Distance, between the fingerprint (Ft) and the fingerprint (Fm); and wherein said second comparison is positive if said distance is less than or equal to a predetermined matching threshold, for example a normalized distance less than or equal to 0.18.

9. The method according to claim 8, further comprising an adaptive update step of the reference PUF fingerprint (Fm), wherein, if the distance calculated in step (f.ii) is between zero and a predetermined update threshold, the reference PUF fingerprint (Fm) stored in the digital token is updated based on a combination, such as a weighted average, of the previous reference fingerprint and the reading fingerprint (Ft), in order to compensate for natural variations of the micro-geometry, said update threshold being lower than said matching threshold.

10. A good, such as a luxury watch, a jewel, a work of art, a handbag or a high-end fashion accessory, characterized by comprising the physical-digital authentication system as defined in any of claims 1 to 6.