(19) DANMARK

(10) DK/EP 3559931 T3

(12) Oversættelse af europæisk patentskrift

Patent- og Varemærkestyrelsen

(51) Int.Cl.: *G 09 C 1/00 (2006.01)* *G 09 C 5/00 (2006.01)* *H 04 L 9/32 (2006.01)*

(45) Oversættelsen bekendtgjort den: **2023-05-30**

(80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2023-04-12**

(86) Europæisk ansøgning nr.: **17822250.1**

(86) Europæisk indleveringsdag: **2017-12-18**

(87) Den europæiske ansøgnings publiceringsdag: **2019-10-30**

(86) International ansøgning nr.: **EP2017083283**

(87) Internationalt publikationsnr.: **WO2018114782**

(30) Prioritet: **2016-12-21 EP 16205920**

(84) Designerede stater: **AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**

(73) Patenthaver: **Merck Patent GmbH, Frankfurter Strasse 250, 64293 Darmstadt, Tyskland**

(72) Opfinder: **ENDRESS, Thomas, Waldsaumstrasse 11, 81377 Muenchen, Tyskland**
Szabo, Daniel, Friedrich Ebert Platz 16, 64289 Darmstadt, Tyskland
Wahl, Fabian, Grosse Grof 8, 9470 Buchs, Schweiz

(74) Fuldmægtig i Danmark: **Plougmann Vingtoft A/S, Strandvejen 70, 2900 Hellerup, Danmark**

(54) Benævnelse: **PUF-BASERET KOMBINERET SIKKERHEDSMARKERING TIL BESKYTTELSE MOD FORFALSKNING**

(56) Fremdragne publikationer:
EP-A1- 2 911 335
EP-A1- 2 999 156
WO-A2-2007/031908
US-A1- 2013 127 959
US-A1- 2015 183 257
PAWAN KUMAR ET AL: "Future prospects of luminescent nanomaterial based security inks: from synthesis to anti-counterfeiting applications", NANOSCALE, vol. 8, no. 30, 1 January 2016 (2016-01-01), pages 14297-14340, XP055382820, United Kingdom ISSN: 2040-3364, DOI: 10.1039/C5NR06965C
O. IVANOVA ET AL: "Unclonable security features for additive manufacturing", ADDITIVE MANUFACTURING, vol. 1-4, 1 October 2014 (2014-10-01), pages 24-31, XP055382782, ISSN: 2214-8604, DOI: 10.1016/j.addma.2014.07.001
WONG CHAU-WAI ET AL: "Counterfeit detection using paper PUF and mobile cameras", 2015 IEEE INTERNATIONAL WORKSHOP ON INFORMATION FORENSICS AND SECURITY (WIFS), IEEE, 16 November 2015 (2015-11-16), pages 1-6, XP032840451, DOI: 10.1109/WIFS.2015.7368579
MIAO WANG ET AL: "Nanomaterial-based barcode", NANOSCALE, , vol. 7 25 May 2016 (2016-05-25), pages 11240-11247, XP002765475, DOI: 10.1039/C5NR01948F Retrieved from the Internet:

Fortsættes ...

URL:http://pubs.rsc.org/en/content/article pdf/2015/NR/C5NR01948F
BORA YOON ET AL: "Recent functional material based approaches to prevent and detect counterfeiting", JOURNAL OF MATERIALS CHEMISTRY C, vol. 1, no. 13, 21 January 2013 (2013-01-21), pages 2388-2403, XP055148122, ISSN: 2050-7526, DOI: 10.1039/c3tc00818e
DANIELA PAUNESCU ET AL: "Particles with an identity: Tracking and tracing in commodity products", POWDER TECHNOLOGY, vol. 291, 29 December 2015 (2015-12-29), pages 344-350, XP055250454, CH ISSN: 0032-5910, DOI: 10.1016/j.powtec.2015.12.035
FEI JIE ET AL: "Drug-laden 3D biodegradable label using QR code for anti-counterfeiting of drugs", MATERIALS SCIENCE AND ENGINEERING C, ELSEVIER SCIENCE S.A, CH, vol. 63, 4 March 2016 (2016-03-04), pages 657-662, XP029489638, ISSN: 0928-4931, DOI: 10.1016/J.MSEC.2016.03.004
F. FAYAZPOUR ET AL: "Digitally Encoded Drug Tablets to Combat Counterfeiting", ADVANCED MATERIALS, vol. 19, no. 22, 19 November 2007 (2007-11-19), pages 3854-3858, XP055382756, DE ISSN: 0935-9648, DOI: 10.1002/adma.200602800
GOOCH JAMES ET AL: "Taggant materials in forensic science: A review", TRAC TRENDS IN ANALYTICAL CHEMISTRY, ELSEVIER, AMSTERDAM, NL, vol. 83, 11 August 2016 (2016-08-11), pages 49-54, XP029729461, ISSN: 0165-9936, DOI: 10.1016/J.TRAC.2016.08.003
NERALAGATTA M. SANGEETHA ET AL: "3D assembly of upconverting NaYF4 nanocrystals by AFM nanoxerography: creation of anti-counterfeiting microtags", NANOSCALE, vol. 5, no. 20, 1 January 2013 (2013-01-01), page 9587, XP055382762, United Kingdom ISSN: 2040-3364, DOI: 10.1039/c3nr02734a
CHEUN NGEN CHONG ET AL: "Anti-counterfeiting with a Random Pattern", EMERGING SECURITY INFORMATION, SYSTEMS AND TECHNOLOGIES, 2008. SECURWARE '08. SECOND INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 25 August 2008 (2008-08-25), pages 146-153, XP031319483, ISBN: 978-0-7695-3329-2
Dr Fred Jordan ET AL: "May/June 2012 PHARMACEUTICAL ENGINEERING anti-Counterfeiting Technologies Identifying Counterfeit Medicines with Industry-Suitable Technologies", , 30 June 2012 (2012-06-30), XP055136117, Retrieved from the Internet: URL:http://www.alpvision.com/pdf/2012_05_P E_Identifying_Counterfeit_Medicines_with_I ndustry-Suitable_Technologies.pdf [retrieved on 2014-08-22]
H Lou ET AL: "The familiar concept of the barcode for tracking may be coming to a chemical reaction near you in the form of coded microparticles", , 1 October 2004 (2004-10-01), XP055382757, Retrieved from the Internet: URL:http://pubs.acs.org/doi/pdf/10.1021/ac 0416463 [retrieved on 2017-06-19]
PETER ZIJLSTRA ET AL: "Five-dimensional optical recording mediated by surface plasmons in gold nanorods", NATURE, MACMILLAN JOURNALS LTD., ETC.|, vol. 459, 21 May 2009 (2009-05-21), pages 410-413, XP007912739, ISSN: 0028-0836, DOI: 10.1038/NATURE08053
JISEOK LEE ET AL: "Universal process-inert encoding architecture for polymer microparticles", NATURE MATERIALS, vol. 13, no. 5, 13 April 2014 (2014-04-13) , pages 524-529, XP055382621, GB ISSN: 1476-1122, DOI: 10.1038/nmat3938
YUHAI ZHANG ET AL: "Multicolor Barcoding in a Single Upconversion Crystal", JOURNAL OF THE AMERICAN CHEMICAL SOCIETY, vol. 136, no. 13, 2 April 2014 (2014-04-02), pages 4893-4896, XP055382626, US ISSN: 0002-7863, DOI: 10.1021/ja5013646
JANGBAE KIM ET AL: "Anti-counterfeit nanoscale fingerprints based on randomly distributed nanowires", NANOTECHNOLOGY, IOP, BRISTOL, GB, vol. 25, no. 15, 20 March 2014 (2014-03-20), page 155303, XP020261704, ISSN: 0957-4484, DOI: 10.1088/0957-4484/25/15/155303 [retrieved on 2014-03-20]
JULIEN ANDRES ET AL: "A New Anti-Counterfeiting Feature Relying on Invisible Luminescent Full Color Images Printed with Lanthanide-Based Inks", ADVANCED FUNCTIONAL MATERIALS, WILEY - V C H VERLAG GMBH & CO. KGAA, DE, vol. 24, no. 32, 27 August 2014 (2014-08-27), pages 5029-5036, XP001591486, ISSN: 1616-301X, DOI: 10.1002/ADFM.201400298 [retrieved on 2014-05-22]
RADZIWON MICHAL ET AL: "Anti-counterfeit Solution from Organic Semiconductor", PROCEDIA ENGINEERING, ELSEVIER, AMSTERDAM, NL, vol. 69, 25 March 2014 (2014-03-25), pages 1405-1409, XP028832760, ISSN: 1877-7058, DOI: 10.1016/J.PROENG.2014.03.135
DAN JIANG ET AL: "Anti-counterfeiting using phosphor PUF", ANTI-COUNTERFEITING, SECURITY AND IDENTIFICATION, 2008. ASID 2008. 2ND INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 20 August 2008 (2008-08-20), pages 59-62, XP031365958, ISBN: 978-1-4244-2584-6

DESCRIPTION

FIELD OF THE INVENTION

[0001] The present invention relates to the field of anti-counterfeit protection of products. Specifically, the invention is directed to a method of reading with a reader device a marking comprising a physical unclonable function, PUF, and a corresponding reader device. In particular, without limitation, such reader device can be used in connection with or can form a component of a multi-component security system, in particular of an anti-counterfeit protection system, which is also disclosed herein as part of an overall security solution for anti-counterfeit protection.

BACKGROUND

[0002] In many industries, counterfeiting of products is a substantial problem that significantly impacts not only the revenues of original product manufacturers, but may even pose a serious threat to health and even life of consumers or operators of counterfeited, i.e. fake products. Such safety relevant product categories include in particular parts for automobiles and aircraft, components for the construction of buildings or other infrastructure, food, and even medical devices and pharmaceuticals.

[0003] In order to limit counterfeiting and address in particular such safety concerns, the industry has developed a number of different protection measures. Broadly used protection measures comprise adding a so-called security feature to a product, the feature being rather difficult to fake. For example, holograms, optically variable inks, security threads and embedded magnetic particles are known security features which are difficult to reproduce by counterfeiters. While some of these security features are "overt", i.e. can be easily seen or otherwise recognized by a user of the product, other security features are "covert", i.e. they are hidden and can only be detected by using specific devices, such as sources of UV-light, spectrometers, microscopes or magnetic field detectors, or even more sophisticated forensic equipment. Examples of covert security features are in particular printings with luminescent ink or ink that is only visible in the infrared part of the electromagnetic spectrum but not in its visible part, specific material compositions and magnetic pigments.

[0004] A specific group of security features, which are in particular used in cryptography, is known as "Physical Unclonable Functions" (PUFs). PUFs are sometimes also referred to as "Physically Unclonable Functions" or "Physical Random Functions". A PUF is a physical entity that is embodied in a physical structure and is easy to evaluate but hard to predict, even for an attacker with physical access to the PUF. PUFs depend on the uniqueness of their physical microstructure, which typically includes a random component that is already intrinsically present in the physical entity or is explicitly introduced into or generated in the physical entity

during its manufacturing and which is substantially uncontrollable and unpredictable. Accordingly, even PUFs being produced by the exact same manufacturing process differ at least in their random component and thus can be distinguished. While in most cases, PUFs are covert features, this is not a limitation and overt PUFs are also possible.

[0005] PUFs are known in particular in connection with their implementation in integrated electronic circuits by way of minimal unavoidable variations of the produced microstructures on a chip within given process-related tolerances, and specifically as being used for deriving cryptographic keys therefrom, e.g. in chips for smartcards or other security related chips. An example of an explanation and application of such chip-related PUFs is disclosed in the article "Background on Physical Unclonable Functions (PUFs)", Virginia Tech, Department of Electrical and Computer Engineering, 2011, which is available in the Internet at the hyperlink http://rijndael.ece.vt.edu/puf/background.html.

[0006] However, also other types of PUFs are known, such as random distributions of fibers in paper used as a substrate for making banknotes, wherein the distribution and orientation of fibers can be detected by specific detectors and used as a security feature of the banknote. In order to evaluate a PUF, a so-called challenge-response authentication scheme is used. The "challenge" is a physical stimulus applied to the PUF and the "response" is its reaction to the stimulus. The response is dependent on the uncontrollable and unpredictable nature of the physical microstructure and thus can be used to authenticate the PUF, and thus also a physical object of which the PUF forms a part. A specific challenge and its corresponding response together form a so-called "challenge-response pair" (CRP).

[0007] Asymmetric cryptography, sometimes also referred to as "public key cryptography" or "public/private key cryptography" is a known technology based on cryptographic system that uses pairs of keys, wherein each pair of keys comprises a public key and a private key. The public keys may be disseminated widely and are usually even publicly available, while the private keys are kept secret and are usually only known to their owner or holder. Asymmetric cryptography enables both (i) authentication, which is when the public key is used to verify that a holder of the paired private key originated a particular information, e.g. a message or stored data containing the information, by digitally signing it with his private key, and (ii) protection of information, e.g. a message or stored data, by way of encryption, whereby only the owner/holder of the paired private key can decrypt the message encrypted with the public key by someone else.

[0008] Recently, blockchain technology has been developed, wherein a blockchain is a public ledger in the form of a distributed database containing a plurality of data blocks and which maintains a continuously-growing list of data records and is hardened against tampering and revision by cryptographic means. A prominent application of blockchain technology is the virtual Bitcoin currency used for monetary transactions in the Internet. A further known blockchain platform is provided for example by the Ethereum project. In essence, a blockchain can be described as a decentralized protocol for logging transactions between parties, which transparently captures and stores any modifications to its distributed database and saves them

"forever", i.e. as long as the blockchain exists. Storing information into a blockchain involves digitally signing the information to be stored in a block of the blockchain. Furthermore, maintaining the blockchain involves a process called "blockchain mining", wherein so-called "miners" being part of the blockchain infrastructure, verify and seal each block, such that the information contained therein is saved "forever" and the block can no longer be modified.

[0009] The public disclosure "Future prospects of luminescent nanomaterial based security inks: from synthesis to anticounterfeiting applications" from PA WAN KUMAR ET AL, NANOSCALE, vol. 8, no. 30, 1 January 2016 (2016-01-01), pages 14297-14340, XP055382820, United Kingdom ISSN: 2040-3364, DOI: 10.1039/C5NR06965C deals with the use of specific luminescent nanomaterial for the use in physical uncloneable function (PUF) devices.

[0010] Additionally it exist several state of the art disclosed in patent documents which deals with similar fields of technology. The three most relevant documents are:
The international patent application WO 2007/031908 A2, which disclosure relates to a physical uncloneable function (PUF) devices for determining authenticity of an item, systems for determining authenticity of a physical item, and methods for determining authenticity of an item. A PUF pattern of the PUF device is damaged when using the item for the first time.

[0011] The European patent EP 2 999 156 B1 on the other hand discloses a system for using printed information, which is viewable from an exterior of a device or a component, the device and the component having mounted thereon a semiconductor chip having a PUF function and an encryption function, and includes auxiliary data, for generating secret information being difficult to duplicate with use of the PUF function, and the secret information, the system comprising a control terminal for reading the printed information, which is viewable, and transmitting the printed information to the semiconductor chip through electronic access means, in which the semiconductor chip further has a tampering determination function of temporarily reconstructing, through the encryption function and the PUF function, the secret information being difficult to duplicate with use of the auxiliary data included in the printed information acquired from the control terminal, performing comparison processing between the secret information included in the printed information and the temporarily-reconstructed secret information being difficult to duplicate, and determining that tampering has occurred when detecting a mismatch between the secret information included in the printed information and the temporarily-reconstructed secret information being difficult to duplicate.

[0012] The European patent application EP 2 911 335 A1 now discloses a device for identifying genuine and counterfeited goods using challenge-response pairs (CRP) based on physical unclonable function (PUF), said device comprising one or more antennae for emitting a number of first electromagnetic signals as challenges to a good and for receiving a number of second electromagnetic signals as responses from the good, both challenge and response forming a challenge-response pair for said good, wherein at least one of the antennae is a wideband antenna, a software defined radio (SDR) unit arranged for emitting said first electromagnetic signal(s) as challenge(s) and arranged for receiving said second

electromagnetic signal(s) as response(s), a challenge-response pair evaluation unit for analysing said challenge-response pair(s) and to provide a result acknowledging if the good is genuine or counterfeit.

[0013] Additionally a method for ANTI-COUNTERFEITING, SECURITY AND IDENTIFICATION is known, from the publication DAN JIANG ET AL: "Anti-counterfeiting using phosphor PUF", which was disclosed on 20 August 2008 at the 2ND INTERNATIONAL CONFERENCE ON IEEE in PISCATAWAY, NJ, USA.

SUMMARY OF THE INVENTION

[0014] The present invention addresses the problem of providing a way of effectively reading a marking of a physical object, such as a product, in order to enable a verification of the authenticity of the object, wherein the marking serves for protecting the object against counterfeiting and tampering and comprises a PUF.

[0015] A solution to this problem is provided by the teaching of the appended independent claims. Various preferred embodiments of the present invention are provided by the teachings of the dependent claims.

[0016] A solution to this problem is provided by the teaching of the appended independent claims. Various preferred embodiments of the present invention are provided by the teachings of the dependent claims.

[0017] Furthermore, a whole security solution is presented herein, including various apparatus' and methods as different aspects that may form part of an overall security solution for effectively protecting physical objects against counterfeiting and tampering.

[0018] A first aspect of the security solution provided herein is directed to a composite security marking for a physical object, in particular an anti-counterfeit composite security marking. The composite security marking comprises a physical unclonable function, PUF, and a representation of a digital signature or of a pointer indicating a location where said digital signature can be accessed. The digital signature digitally signs a hash value resulting from application of a predetermined cryptographic hash function to data representing a response generated by the PUF in reaction to a challenge of a predetermined challenge-response authentication scheme.

[0019] The term "physical object", as used herein, refers to any kind of physical object, in particular to any kind of man-made or product or natural object, such as a vegetable or a piece of a natural raw material. Furthermore, as used herein, the term "physical object" may also refer to a person or an animal to which a composite security marking may be applied. A physical object may itself comprise multiple parts, e.g. a consumable good and a packaging thereof.

[0020] The term "composite security marking", as used herein, refers to a physical entity that comprises at least two different individual markings as its components, (hence "composite"), is adapted to be applied to or created on or in a physical object, and remains accessible after being applied or created on or in the physical in order to evaluate it. In the composite security marking according to the above first aspect of the security solution, a first component is a PUF and a second component is a representation of a digital signature or of a pointer indicating a location where said digital signature can be accessed. In particular, the two or more components of the composite security marking may be located on or within a same substrate or part of the physical object. Alternatively, a subset of the components or all of them may be located on or within separate substrates or other parts of the physical object.

[0021] The term "digital signature", as used herein, refers to a set of one or more digital values that confirms the identity of a sender or originator of digital data and the integrity of the later. To create a digital signature, a hash value is generated from the data to be protected by way of application of a suitable cryptographic hash function. This hash value is then encrypted with a private key (sometimes also called "secure key") of an asymmetric cryptographic system, e.g. based on the well-known RSA cryptographic system, wherein the private key is typically known only to the sender/originator. Usually, the digital signature comprises the digital data itself as well as the hash value derived from it by the sender/originator. A recipient may then apply the same cryptographic hash function to the received digital data, use the public key corresponding to said private key to decrypt the hash value comprised in the digital signature, and compare the decrypted hash value from the digital signature to the hash value generated by applying the cryptographic hash function to the received digital data. If both hash values match, this indicates that the digital information has not been modified and thus its integrity has not been compromised. Furthermore, the authenticity of the sender/originator of the digital data is confirmed by way of the asymmetric cryptographic system, which ensures that the encryption using the public key only works, if the encrypted information was encrypted with the private key being mathematically paired to that public key.

[0022] The term "cryptographic hash function", as used herein, refers to a special type of hash function, i.e. a mathematical function or algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash value), which is designed to also be a one-way function, i.e. a function that is easy to compute on every input, but hard to invert given the image of a random input. Preferably, the cryptographic hash function is a so-called collision resistant hash function, i.e. a hash function that is designed such that it is difficult to find two different data sets d1 and d2 such that hash(d1) = hash(d2). Prominent examples of such hash functions are the hash functions of the SHA-family, e.g. the SHA-3 function or the hash functions of the BLAKE family, e.g. the BLAKE2 function. In particular, so-called "provably secure cryptographic hash functions" may be used. These are hash functions for which a certain sufficient security level can be mathematically proven. In the present security solution, the security of the cryptographic hash function is further improved by the fact, that the reading of a marking comprising a PUF, particularly of a composite security marking, as disclosed herein, takes place at a particular location and time, where the physical object bearing the marking is

actually present at such location and time. This can be used either to increase the absolute level of security that can be achieved or to allow for the use of cryptographic hash functions working with smaller data sets, e.g. shorter data strings as inputs and/or outputs, while still providing a given required security level.

[0023] A "pointer indicating a location where said digital signature can be accessed", as used herein, may be in particular a pointer to a local or remote database or to a server address or Internet address, e.g. a hyperlink or similar, at which the digital signature can be accessed, e.g. downloaded. The pointer may particularly be implemented using an RFID transmitter or a single- or multi-dimensional barcode, such as a QR-Code or a DATAMATRIX-code.

[0024] The composite security marking according to the first aspect of the present security solution can be used by a first party, e.g. an originator of a physical object in the form of a product, to protect any physical object to which the components of the marking, i.e. at least a respective PUF and the corresponding digital signature of its response, can be applied. In particular, the marking is preferably applied to the physical object in such a way, that it cannot be separated again from the object without destroying the marking or at least parts thereof.

[0025] Already by nature, the PUF is "unclonable" and thus provides a first level of security, i.e. as a means of confirming the authenticity of the marking and thus of the physical object. This first security level is, however, further enhanced to a higher second security level by the combination of the PUF with the digital signature that cryptographically signs a hash value derived from a response by the PUF to a challenge of a predetermined challenge-response-scheme pertaining to the PUF. In this way, in analogy to a digital signature for electronic documents, a digital signature for physical objects is created for protecting such objects, particularly against counterfeiting.

[0026] In order to verify the authenticity of the physical object respectively its origin, a challenge according to this challenge-response-scheme is applied by a second party receiving the physical object to the PUF of the physical object's marking and the same cryptographic hash function is applied to generate a respective hash value from data representing the response received from the PUF. The hash value contained in the digital signature can be derived by decrypting the digital signature using its related public key and then the two hash values can be compared. If they match, this indicates that the physical object is authentic and the composite security marking has not been tampered with. Otherwise, i.e. if they do not match, this indicates that some sort of fraud might have happened since the originator applied the composite security marking to the physical object.

[0027] Accordingly, the composite security marking provides an additional level of security, and thus an improved way of protecting a physical object against counterfeiting and tampering. Furthermore, as the response of the PUF to a challenge according to the challenge-response-scheme yields digital data, e.g. a data string, the composite security marking can be used to protect any physical object to which such marking can be applied, even if the object itself does not provide any digital data.

[0028] In the following, preferred embodiments of the composite security marking are described, which can be arbitrarily combined with each other or with other aspects of the solution described herein, unless such combination is explicitly excluded, inconsistent or technically impossible.

[0029] According to a first preferred embodiment the PUF comprises an up-converting dye (UCD), preferably a plurality of different converting dyes. A UCD is a dye that shows the effect of photon up-conversion (UC), which is a process in which the sequential absorption of two or more photons leads to the emission of light at shorter wavelength than the excitation wavelength. It is an anti-Stokes-type emission. A typical example for such a process is the conversion of infrared light to fluorescent visible light. Materials by which up-conversion can take place often contain ions of d-block and f-block elements of the periodic system. Examples of these ions are Ln3+, Ti2+, Ni2+, Mo3+, Re4+, Os4+, and so on. Such materials typically comprise a relatively low portion of vibrionic spectral broadening and thus show fluorescence in very narrow bands of the electromagnetic spectrum. Using a variety of different combinations, i.e. mixes, of various up-converting substances, it is possible to generate huge number of distinguishable individual spectrums.

[0030] For example, assuming a spectral resolution of 20 nm within the spectral region of 400 nm to 800 nm, there are already 2^{20} different possibilities, if the detection is limited to the binary question of whether or not the spectrum shows a peak within the respective 20 nm interval. In other words, a binary value of "0" or "1" may be assigned to each interval, one of these values indicating presence of a peak in that interval and the other value indicating absence of such peak. Accordingly, a digital string can be formed from the 20 binary values assigned to the 20 intervals into which said spectral region is divided and thus 2^{20}, i.e. approximately 10^6 different combinations can be represented by such string. If instead an interval of only 10 nm is used, the numbers increased to 2^{40}, i.e. approximately 10^{11} different combinations. If in addition, in each interval further distinction is made in case of each peak, e.g. whether the respective peak is closer to a "full" peak or to only a "half" peak (cf. Fig. 4 (b)), then in the case of 40 intervals the number of combinations is even increased to 3^{40}, i.e. approximately 10^{18} combinations. Accordingly, it is virtually impossible, to create a mix of UCDs in such a way, that it shows the same spectrum, as the original mix it seeks to clone.

[0031] In this way, UCDs can be used to create a PUF. An advantage of using UCDs for PUFs is that they can be applied to almost any physical object, e.g. as a component of a coating or a material from which the physical object or parts thereof are made. Furthermore, UCDs are typically covert features and cannot be easily recognized without sophisticated equipment. This can be used to further increase the achievable security level.

[0032] According to another preferred embodiment the PUF comprises an unclonable physical pattern or a structure configured to generate a virtual pattern in response to the challenge. In one variant of this embodiment, the pattern may comprise a huge number of microscopic

particles the location and/or orientation of which represent an uncontrollable and unpredictable physical pattern that can be detected but not cloned by practical means. In another preferred variant, said structure configured to generate a virtual pattern comprises a microstructure being configured to create an optical speckle pattern when illuminated with light of a suitable light source. In particular, the microstructure may comprise a plurality of so-called quantum dots, i.e. very small semiconductor particles, which are only several nanometers in size, so that their optical and electronic properties differ from those of larger particles and which emit light of specific wavelengths if electricity or light is applied to them (i.e. as a challenge). The quantum dots' size, shape and material, which can be controlled during manufacturing, determine these wavelengths, and thus a huge variety of different emission spectrums can be created as responses of a related challenge-response-scheme. In another preferred variant, the microstructure may comprise a plurality of rod-shaped quantum materials (quantum rods), which offer a similar color conversion mechanism and extended color gamut as spherical quantum dots. The unique advantage of quantum rods is the emission of polarized light. Of course, also combinations of the above variants of microstructures are possible.

[0033] The term "light" as used herein, refers to electromagnetic radiation and may include, without limitation, radiation in the visible part of the electromagnetic spectrum. Light may for example also comprise ultraviolet or infrared radiation instead or in addition to visible radiation. A "speckle" pattern is an intensity pattern produced by the mutual interference of a set of many electromagnetic wavefronts of a same or similar wavelength, e.g. in the visible spectrum, but different phases and usually also different amplitudes. The intensity of the waves resulting from the interference varies randomly, at least in the spatial dimension. Typically, monochromatic and sufficiently coherent radiation, such as laser emission, is used for generating such speckle patterns.

[0034] In particular, the microstructure can be an integral microstructure such as a surface of a physical object showing a sufficient optical roughness, or it can comprise a plurality of separate parts, e.g. microscopic particles in a random distribution within a body (which is at least partially transparent to the radiation) or on a surface of a physical object.

[0035] Similar as for UCDs, an advantage of using such speckle-generating microstructures for PUFs is that they can be applied to almost any physical object, be it on its surface or even embedded within the object, if the latter is sufficiently transparent to the light needed to generate the speckle pattern. Because such microstructures typically have characteristic dimensions in the order of the wavelengths of the light, they may be made very small and are thus also typically covert features that cannot be easily recognized without sophisticated equipment. This again increases the achievable security level.

[0036] According to a further preferred embodiment, the PUF comprises at least one of the following: (i) an image in which hidden information is steganographically embedded; (ii) an image that is printed with an ink containing one or more types of up-converting dyes, UCD; (iii) a hologram containing hidden phase-coded or frequency-coded information. In particular, in addition to the above-mentioned covert security features, which increase the security level that

can be achieved, the image respectively hologram may comprise or represent in addition an overt feature, e.g. a one-dimensional or multi-dimensional barcode, such as a OR-Code or DATAMATRIX-Code, in order to present further information. For example, such a code may overlay the image or hologram below that contains the covert feature or the image may be printed with ink containing a mix of UCDs. This allows for very space efficient implementations of PUFs comprising both covered security aspects and overt security features or other information, such as the digital signature of the composite security marking or product codes, manufacturer identities, production site information etc..

[0037] According to a further preferred embodiment, the representation of the digital signature and/or the pointer is implemented by one or more of the following: (i) an alphanumeric string; (ii) a graphical or image representation; (iii) a one-dimensional or multi-dimensional barcode; (iv) a device, e.g. a short-range wireless chip, such as an RFID chip, transmitting a signal carrying the representation of the digital signature or pointer. In particular, this embodiment may be combined with the immediately preceding embodiment. Furthermore, the digital signature and/or pointer may be represented by only a part of said string, graphical image representation, barcode or signal, respectively, each of which may in addition represent further information that may or may not be security related.

[0038] According to a further preferred embodiment, the composite security marking comprises said pointer and said pointer indicates a routing to a server from which the digital signature can be retrieved. In particular, this allows for a central management of the digital signatures of multiple physical objects in a server environment. Furthermore, this enables a centralized monitoring and control of the use of the managed digital signatures which can be used in many ways, for example for early detection of fraud attempts or supply chain optimization. Specifically, a trust center infrastructure may be used for such centralized monitoring and control. Optionally, the pointer may also contain or point to information regarding a product type, serial number or other information relating to the physical object being marked with a composite security marking.

[0039] According to a further preferred embodiment, wherein the PUF comprises a UCD, said data representing a response generated by the PUF in reaction to a challenge of a predetermined challenge-response authentication scheme for said UCD represents a spectral barcode having a continuous or a quantized range of allowed spectral values for a selected discrete subset of wavelengths, and/or a characteristic lifetime of a luminescence effect occurring in the response. This allows in particular for a determination and scaling of the number of bits or other information units that can be encoded by using the UCD of the PUF. If, for example, in each interval of the spectrum the corresponding spectral value is quantized into one of four spectral levels, that interval of the spectrum can be used to code two bits of information represented by the PUF. Adding also a quantization of the characteristic lifetime of the luminescence effect in that spectral interval, can be used to add further bits of information. A quantization can be preferable over a continuous range of allowed spectral values, as it may increase the robustness against distortions of the response generated by the PUF.

[0040] According to a further preferred embodiment, wherein the PUF comprises an unclonable physical pattern or a structure configured to generate a virtual pattern in response to the challenge, said data representing a response generated by the PUF in reaction to a challenge of a predetermined challenge-response authentication scheme for said unclonable physical pattern or structure configured to generate a virtual pattern represents at least one recognized aspect or portion of said physical pattern or said virtual pattern, respectively. In particular, said recognized aspect might relate to a statistical measure applied to the physical pattern or virtual pattern, such as an average distance between individual nodes of the pattern, a related variance or standard deviation, or any other statistical moment. Alternatively, according to another variant, said pattern may be scanned, e.g. in a matrix fashion, and thus converted into a string of bits, e.g. by using a discrimination threshold and representing matrix points showing a light intensity above the threshold by a "1" and all matrix points having a light intensity below the threshold as "0", or vice versa. In this way, patterns can be efficiently converted into data representing a response generated by the PUF in reaction to the corresponding challenge.

[0041] According to a further preferred embodiment, the composite security marking comprises at least one component resulting from an additive manufacturing process and the PUF is contained in or otherwise forms part of that component. In particular, the additive manufacturing process may be so-called 3D-printing process. Preferably, the PUF is provided already in the raw material, from which the component is made using the additive manufacturing process. In this way, the PUF can be introduced into the component without a need for modifications to the manufacturing data based on which the additive manufacturing process is performed. Furthermore, the extremely high flexibility and complexity provided by additive manufacturing methods, allows for a virtually endless variety of different PUFs and their arrangement on or within the physical object to be marked. This, again, can be used to further increase the security level that can be achieved with the composite security marking.

[0042] A second aspect of the solution provided herein is directed to a physical object, in particular a product, comprising a composite security marking according to the first aspect of the solution, preferably according to any one or more of its embodiments or variants described herein.

[0043] Specifically, according to preferred embodiments, the physical object is a product comprising one or more items for consumption or use and a packaging thereof, and the PUF of the composite security marking is arranged on or contained within at least one of the items for consumption or use, while the representation of or pointer to the digital signature is arranged on or within the packaging. Thus, in this embodiment, the composite security marking is formed on two different substrates. This might be advantageous especially in situations, where there is not enough space on the product itself to carry both the PUF and the digital signature. In one variant, the product is a pharmaceutical product comprising for example a bottle containing a liquid pharmaceutical or a blister pack containing tablets as an item for consumption and a cardboard box surrounding the bottle or blister pack as a packaging. The PUF of the composite security marking is a printed label placed on the bottle wherein the label

is printed with an ink containing a secret mix of different UCDs. The digital signature corresponding to the PUF is be printed on the packaging in the form of a two-dimensional barcode, e.g. a OR-code or a DATAMATRIX code.

[0044] According to further preferred embodiments, the physical object comprises one or more of the following items for consumption (consumable goods) or use: a pharmaceutical or cosmetic compound or composition; a medical device; a laboratory equipment; a spare part or component of a device or system; a pesticide or herbicide; a seeding material; a coating, ink, paint, dye, pigments, varnish, impregnating substance, functional additive; a raw material for additive manufacturing of products. In particular, all of these items have in common that there is a need to prevent counterfeiting, in order to avoid malfunctions, health threats or other risks.

[0045] A third aspect of the solution provided herein is directed to a method of providing a physical object, in particular a product, with a composite security marking. The method comprises the following steps: (i) adding a physical unclonable function, PUF, to an object to be marked; (ii) applying a challenge of a predetermined challenge-response authentication scheme to at least one of said added PUFs to trigger a response according to said authentication scheme in reaction to said challenge; detecting said response; (iii) applying a predetermined cryptographic hash function to data representing said response to obtain a hash value; (iv) signing said hash value with a digital signature; and (v) adding a representation of the digital signature or a pointer indicating where the digital signature can be accessed to the object to be marked. Accordingly, a composite security marking is provided to the physical object, which comprises said PUF and its corresponding digital signature or a pointer thereto. Preferably, the PUF is a PUF as described above as a component of a composite security marking according to the first aspect of the present security solution, respectively its preferred embodiments and variants. The produced composite security marking produced by the method thus corresponds in particular to the composite security marking according to the first aspect of the present security solution. Preferably, the method further comprises generating a public/private key pair of an asymmetric cryptographic system and using the private key for creating said digital signature of said hash value and making said corresponding public key available, directly or indirectly, to a recipient of the object bearing the composite security marking.

[0046] Optionally, the composite security marking may comprise more than one PUF, particularly such as described above, and more than one digital signature derived from a PUF or a pointer thereto according to steps (ii) to (v), as described above. Accordingly, in a corresponding embodiment of a method, the additional digital signatures may be derived either by applying in step (ii) different challenges corresponding to different challenge-response-schemes to the same PUF, if supported by the latter, or by adding in step (i) two or more PUFs to the object to be marked and performing step (ii) for each of these PUFs. In both of these variants, steps (iii) through (v) follow for each of the responses, wherein for step (v) the pointer may point to the corresponding set of generated digital signatures. In this way, the achievable security level may be increased even further.

[0047] According to a further preferred related embodiment, the step of adding one or more PUFs to an object to be marked comprises one or more of the following: (a) adding one or more PUFs to a coating material to obtain a PUF-enhanced coating material and applying, e.g. by spraying, coating, infiltrating, printing or painting, the PUF-enhanced coating material to a physical object to be marked; (b) adding one or more PUFs, preferably by means of one or more chemical or mixing processes, to a raw material or an intermediate material, such as an ink or color, before or while producing thereof a physical object to be marked; (c) adding one or more PUFs to a raw material or fusion agent of an additive manufacturing process, e.g. 3D-printing process, for producing a physical object to be marked or at least a part of such object. In particular, the one or more PUFs may be added to the raw material or fusion agent before or during the additive manufacturing process. This allows an easy integration of the one or more PUFs into the object itself. Furthermore, the security level can be further increased, because as the one or more PUFs this become an integral component of the object, a removal, in particular a non-destructive removal, of the one or more PUFs from the object, can be effectively prevented.

[0048] A fourth aspect of the solution provided herein is directed to an apparatus for providing a physical object, in particular a product, with a composite security marking, wherein the apparatus is adapted to perform the method according to third aspect of the solution, preferably according to any one or more of its embodiments or variants described herein. Accordingly, the description and advantages of the third aspect of the solution applies mutatis mutandis to the apparatus according to this fourth aspect.

[0049] A fifth aspect of the solution described herein is directed to a method of reading with a reader device a marking comprising a physical unclonable function, PUF. The method comprises the following steps: (i) a stimulation step, wherein a physical challenge according to a predetermined challenge-response authentication scheme corresponding to the PUF is created and applied to a PUF; (ii) a detection step, wherein a response generated by the PUF in accordance with the challenge-response authentication scheme in reaction to the challenge is detected and a digital signal representing the response is generated; (iii) a processing step, wherein the digital signal is processed in order to generate a hash value of the response by application of a predetermined cryptographic hash function to the digital signal, and (iv) an output step, wherein data representing the generated hash value as a first reading result is output.

[0050] The term "stimulation", as used herein, refers to creating and applying to a PUF a physical challenge according to a predetermined challenge-response authentication scheme corresponding to the PUF. Specifically, a stimulation may comprise emitting electromagnetic radiation as a challenge that triggers a response according to the challenge-response authentication scheme, when it is applied to a PUF being sensitive to this particular radiation, e.g., if the PUF is a UCD at which an anti-Stokes effect generating the response can be triggered by said radiation. Accordingly, a "stimulator", as used herein, is a component of the reader device being adapted to create such stimulation and apply it to a PUF.

[0051] The term "detection of a response generated by a PUF", as used herein, refers to physically detecting a response generated by a PUF in reaction to a challenge in accordance with a corresponding challenge-response authentication scheme and generating a digital signal representing the response, e.g. by respective data being carried by the digital signal. Accordingly, a "PUF-detector", as used herein, is a component of the reader device being adapted to perform the detection step. In particular, the PUF-detector may comprise a receiver for electromagnetic radiation being emitted by the PUF in response to the challenge applied to it by a stimulator.

[0052] In order to apply the predetermined cryptographic hash function to the digital signal, the hash function may particularly act on the whole digital signal, e.g. a data representation of the complete digital signal, or only to a distinctive portion thereof, such as for example (i) a payload portion (or a distinctive subset thereof) of a digital signal being represented according to a communication protocol defining an overhead portion and a payload portion of the signal, or (i) a portion of such signal falling into a specific time frame, e.g. into a defined time period following a start of the detection following application of the challenge to a PUF.

[0053] Accordingly, the method of reading according to this aspect of the solution can be advantageously used to "read" markings comprising a corresponding PUF and provide the "reading" result as output data that can be used to verify whether or not the marking, or a physical object bearing the marking has been counterfeited or tampered with. In particular, the method may be used to "read" a composite security marking according to the first aspect of the solution, for example according to any one or more of its embodiments or variants described herein. Thus, the method of reading can form part of an overall solution that provides an additional level of security, and thus an improved way of protecting a physical object against counterfeiting and tampering.

[0054] According to a preferred embodiment, the digital signal is generated in the processing step in such a way that it represents at least one PUF-specific distinctive property of the response that is, at least substantially, invariant under variations of the environmental conditions at which the response is detected. By way of example, such varying environmental conditions could be light conditions, temperature, air pressure or other parameters or properties of the environment to which the PUF is typically exposed during it being detected by the reader device. An advantage of this embodiment is an increased robustness of the method of reading and the reader device used therefore with respect to their capability of correctly reading markings comprising a corresponding PUF. This enables an even more reliable distinction between counterfeited or tampered markings and physical objects bearing such markings on the one hand, and markings/objects that have not been counterfeited or tampered with on the other hand.

[0055] According to a further preferred embodiment, detecting the response in the detection step comprises detecting at least one property of electromagnetic radiation emitted by the PUF as a response in reaction to the challenge and generating the digital signal such that it represents this response. This allows, in particular, for a contactless, wireless reading of a

marking containing the PUF. Such a method of reading and a respective reading device can particularly be advantageously used to detect responses of PUFs that are very small or embedded under a surface of a marking/object or where the marking or the physical object bearing the marking is very sensitive to mechanical or chemical impacts that would typically go along with a contact-based reading method.

[0056] Specifically, according to a further and related embodiment, detecting the response in the detection step comprises detecting a characteristic lifetime of a luminescence effect occurring in the response as a property of electromagnetic radiation emitted by the PUF. Accordingly, the detection step may particularly comprise detecting the luminescent radiation at different subsequent points in time after a stimulation of a corresponding PUF in order to derive from the detected radiation a measure for a characteristic lifetime, such as a half-time or other measures of a decay time, for example. As such characteristic lifetimes of luminescence effects are mainly only material specific, they are invariant under a large variety of different environmental parameters and are therefore particularly suitable for characterizing the response of a corresponding PUF showing such an effect as a distinctive property.

[0057] According to a further related preferred embodiment detecting the response in the detection step comprises detecting a spectrum of the emitted radiation as a property of electromagnetic radiation emitted by the PUF. Furthermore, processing the digital signal in the processing step comprises determining from the digital signal one or more of the following: (i) the position (i.e. wavelength or frequency or a related parameter) of one or more characteristic features (e.g. peaks, gaps or minima within the spectrum); (ii) one or more statistical measures characterizing the spectrum (e.g. mean, median, variance, standard deviation or other statistical moments or measures); (iii) one or more quantized spectral values of the spectrum (e.g. of the detected intensities within an intensity spectrum of the radiation); (iv) a spectral barcode representing a continuous or a quantized range of allowed spectral values occurring in the spectrum, e.g. for a selected discrete subset of wavelengths. Also each of these variants may provide an increased robustness of the method against varying environmental conditions at which the response is detected.

[0058] According to a further preferred embodiment, the method further comprises an acquisition step, wherein a composite security marking comprising a PUF and a corresponding first digital signature or a pointer indicating a source where such first digital signature can be accessed is read, and said first digital signature is acquired from the marking or the source indicated by the pointer, respectively. In addition, in the output step (i) a representation of the acquired first digital signature, and/or (ii) a matching output indicating whether, according to at least one predetermined matching criterion, a hash value provided and signed by the acquired first digital signature matches the hash value generated from the response to the challenge, is output. In this way, the method provides a verification of the authenticity of the marking, respectively of the physical object bearing the marking by allowing for a comparison, e.g. by user, between the first digital signature comprised in the marking on the one hand, and a corresponding representation of information contained in the response of the PUF of the marking on the other hand. Furthermore, according to the second alternative (ii) such

comparison, i.e. matching, is already available as part of the method itself, which further increases the reliability and ease-of-use of this method. In particular, the composite security marking may be a marking as described herein in connection with the first aspect of the present security solution, e.g. according to one or more of its preferred embodiments and variants described herein.

[0059] According to a further preferred embodiment the acquisition step further comprises acquiring from the composite security marking a second digital signature or a pointer indicating a source where a particular second digital signature pertaining to the marking can be accessed. Furthermore, the output step further comprises outputting a representation of the acquired second digital signature as a second reading result. In particular, the composite security marking may be a marking as described herein in connection with the first aspect of the present security solution, e.g. according to preferred embodiments and variants thereof as described herein, where an object being marked by the marking is a product comprising one or more items of consumption or use and a packaging thereof. This embodiment enables the reader device to acquire, in addition to the response, further information comprised in the marking, which may particularly be supply chain information. On the one hand, this can be used for both (i) examining the marking/object in view of whether it has been counterfeited or tampered with, or not, and (ii) reading and outputting additional information, such as supply-chain or other logistics information. Furthermore, however, the combination of both uses (i) and (ii) can be utilized to further increase the security aspect of the present security solution, because such additional information, like supply chain information, can be used to retroactively identify locations or persons being involved in supply chain, where a potential fraud might have happened as well as potential related dates or time frames. Accordingly, a reader device adapted to perform the method of this embodiment is a dual-use or even multi-use device, which increases the ease of use and reduces the number of different devices needed to read the complete composite security marking.

[0060] According to related preferred embodiments the second reading result comprises one or more of the following information: (i) location information pertaining to a location where the second digital signature was acquired by the reader device; (ii) authentication information of a user of the reader device; (iii) time and/or date information indicating the point in time at which the second digital signature was acquired by the reader device; (iv) a product identification, serial number, and/or batch number of an object being marked by the marking; (v) an expiration date of an object being marked by the marking.

[0061] According to a further preferred embodiment the output step further comprises outputting at least a part - preferably the whole - of a reading result in the form of a one-dimensional or a multi-dimensional barcode. This enables the use of readily available barcode scanners for the further processing of the output provided by the output step, which may be particularly advantageous, where the reader device is integrated within or interacting with an automated production line or other processing line, where its outputs need to be further processed by algorithms processed by the line rather than by a human user.

[0062] According to a further preferred embodiment, the method further comprises an authentication step, wherein a user is authenticated before permitting him or her to further operate the reader device in case of a successful authentication. This can be advantageously used to further increase the security of the solution by preventing unauthorized users from successfully interacting with the reader device and thus getting involved in the security chain provided by the present security solution. Furthermore, this can be used to acquire user identity or other user related information, which can be used to increase the transparency of the flow of physical objects being marked by the marking, particularly products, along a supply chain. In case of security concerns, this information can then be used to track down potential threats to the security provided by the overall solution and to identify locations or persons which might be related to such threats.

[0063] According to a further preferred embodiment, the method further comprises a communication step, wherein a reading result is communicated over a communication link to an opposing side. Particularly, the communication step might be adapted for sending and receiving data over a wireline, wireless, or optical communication link, such as by way of example and without limitation a communication link based on wireless LAN, Bluetooth, cellular network or a classical telephone line. Such communication link may be used for a variety of different purposes, including for sending acquired information, e.g. the output provided in the output step, to an opposing side, which might for example be a central security instance, such as a trust center comprising a central security server, which might form a component of the present security solution.

[0064] Furthermore, according to a further embodiment, the communication step further comprises capturing and sending security-related information to a predetermined opposing side over the communication link. Said opposing side might for example be the trust center mentioned in the immediately preceding embodiment. In particular, such sending of security-related information may occur randomly, or may be specifically triggered according to a predetermined trigger scheme or remotely, e.g. by the opposing side. This allows for a remote monitoring of the security status of the reader device itself, and/or of security-related events the reader device is involved in. Such a security-related event might for example be a detection of a marking/object that has been counterfeited or tampered with, according to the output generated in the output step or other security-related information provided by the reader device.

[0065] Specifically, according to related preferred embodiments, the security-related information comprises one or more of the following: (i) location information characterizing a current or past location of the reader device; (ii) user data characterizing or identifying a user of the reader device; (iii) network data characterizing the communication link; (iv) information characterizing an attempt or actual act detected by at least one sensor of the reader device or a corresponding reaction of the reader device (e.g. as described above); (v) authentication information generated by an authentication device provided in the reader device, preferably by the authentication device described above.

[0066] According to a further embodiment, the method further comprises an information monitoring step, wherein a security event is detected in information contained in a signal received from the opposing side over the communication link. This step enables, in particular, a transition of the reader device into a safe mode or even its deactivation, in case an authorized opposing side, e.g. a central security center, sends information containing such security event to the reader device, in order to avoid any negative impact the reader device might otherwise have on the overall security system. Such negative impact might result, for example, if any compromising act such as an unauthorized intrusion or firmware/software modification at the reader device or a use by an unauthorized person or at an unauthorized location has occurred and been communicated to or otherwise detected by the opposing side.

[0067] According to a further preferred embodiment, the method further comprises an access monitoring step, wherein one or more of the following are detected by means of one or more sensors as a security event: (i) an attempt or actual act of physical intrusion into the reader device, such as an opening of its housing; (ii) an attempt or actual act of locally or remotely accessing an internal control functionality of the reader device, e.g. its firmware, operating system or an application, wherein such access is not available to a user of the device in the course of its normal operation. Specifically, such attempted access might be directed to taking over control of the functionality of the reader device or to modifying same. Consequently, this embodiment may be advantageously used to further increase the security aspect of the present security solution, and particularly to protect both the reader device itself and the whole solution presented herein against unauthorized intrusion and tampering.

[0068] According to a further related preferred embodiment, the method further comprises a security defense step, wherein one or more of the following security measures are performed in reaction to detection of a security event: (i) locking the reader device such as to limit or prevent its further use; (ii) self-destroying at least one functional part of the reader device or destroy data stored therein in order to prevent its further use or access by a user; (iii) output an error message. In particular, the security measures may be considered specific measures for turning the reader device into a safe or mode or for deactivating it, as described above.

[0069] According to a further preferred embodiment, the outputting step comprises digitally signing data containing the generated hash value and outputting the resulting digital signature as the first reading result. In this way, the method can be used particularly to initially generate a digital signature of a response generated by a PUF in reaction to a challenge of a predetermined challenge-response authentication scheme, e.g. during a manufacturing or commissioning process of products to be protected by a composite security marking, as disclosed herein. In particular, the generated digital signature can be incorporated in addition to the PUF into such composite security marking. Preferably, the method, e.g. the outputting step, further comprises generating a public/private key pair of an asymmetric cryptographic system and using the private key for creating said digital signature of said hash value and making said corresponding public key available, directly or indirectly, to a recipient of the object bearing the composite security marking.

[0070] According to a further preferred embodiment, the method further comprises a storage step, wherein a reading result being output in the output step is stored into a block of a blockchain. This enables a secure, reliable storage of the reading results with very high data integrity, such that it is essentially impossible to manipulate or erase or otherwise taper with or lose such data, e.g. due to unintended or deliberate deletion or due to data corruption. Thus, the complete reading history remains available. Furthermore, the stored information can be accessed wherever access to the blockchain is available. This allows for a safe and distributed storage and access to the stored reading results, e.g. for integrity verification purposes such as checking whether a supplier of a product being marked with a composite security marking, as described herein, was in fact the originator of the product, or not. Based on this embodiment, the physical world, to which the marked objects and the markings themselves belong, can be connected to the power of blockchain technology. Thus, a high degree of traceability of the origin and supply chain of physical objects, such as products, can be achieved.

[0071] According to a further related preferred embodiment the storage step comprises: (i) storing a first reading result comprising data representing the hash value generated in the processing step into a block of a first blockchain; and (ii) storing the second reading result obtained in the acquisition step (as described above), into a block of a second blockchain being separate from the first blockchain. This allows for storing and thus saving both the first and second reading results, i.e. the one being derived from reading the PUF and the one being read from the second digital signature, into a blockchain, thus providing the advantages discussed in connection with the immediately preceding embodiment. Using different blockchains for the two different reading results further provides the advantage of easily supporting a combination of an existing (second) supply chain for the second reading results with an additional first supply chain, for the first reading results related to the responses of the PUFs. Accordingly, different access rights can be easily enabled and the management of the blockchains can be in the hands of different authorities. In particular, this embodiment can be used to verify whether (i) a supplier of a product was in fact its originator, and (ii) whether the supply chain was as expected, or not.

[0072] According to a further related preferred embodiment the storage step further comprises: (i) when storing the first reading result in a block of the first blockchain, including a cross-blockchain pointer, which logically maps the block of the first blockchain to a corresponding block of the second blockchain into the block of the first blockchain; and (ii) when storing the second reading result in a block of the second blockchain, including a cross-blockchain pointer, which logically maps the block of the second blockchain to a corresponding block of the first blockchain into the block of the second blockchain. In this way, the two blockchains can be interconnected by the cross-blockchain pointers which can be used to further increase the achievable security level of the present security solution. In particular, this can be used to track down attempts of tampering with or counterfeiting marked objects at different points along a supply chain. For example, this embodiment allows for tracking down a location and/or a point in time of such an attempt or, in case of a mandatory authentication at the reader device, an identification of a user being involved with such an attempt.

[0073] A sixth aspect of the present security solution is directed to a reader device for reading a marking comprising a physical unclonable function, PUF, wherein the reader device is adapted to perform the method of the fifth aspect of the present security solution, preferably, according to anyone or more of its embodiments and variants described herein. Therefore, what is described herein about the fifth aspect of the present security solution similarly applies to the reader device according to this sixth aspect.

[0074] Specifically, the reader device may comprise as functional units (i) a stimulator being configured to perform the stimulation step; (ii) a PUF-detector being configured to perform the detection step; (iii) a processing device configured to perform the processing step; and (iv) an output generator being configured to perform the outputting step.

[0075] According to preferred embodiments, the reader device may further comprise one or more of the following: (v) an acquisition device configured to perform said acquisition step; (vi) an authentication device configured to perform said authentication step; (vii) a communication device configured to perform said communication step; (viii) a monitoring device configured to perform said information monitoring step; (ix) a security device comprising at least one sensor and being configured to perform said access monitoring step; (x) a security defense arrangement being configured to perform said security defense step; (xi) a blockchain storing device configured to perform said storage step. Preferably, two or more of components (i) to (xi) may be combined or integrated into a multi-functional component of the reader device. For example, all components involving a processing of data, might be combined into or implemented as an integral multi-functional processing unit.

[0076] According to further preferred embodiments, the reader device is integrated or otherwise forms a component of one or more of the following: a handheld device, e.g. a product or barcode scanning device; a production, quality control or commissioning equipment; a production or quality control or commissioning line; a flying object, e.g. a drone; a robot, e.g. an agricultural robot; an agricultural machine. This allows for an integration of the reader device's functionality into a system having additional or broader functionality, particularly in an automated or semi-automated manner. For example, in the case of a production quality control or commissioning line the reader device may be integrated into the line in such a way that it automatically reads the markings, in particular composite security markings, on the products running along the line in order to perform an initial capturing of the related data. That captured data may then be stored into a related database or compared to already stored data for the sake of verifying that the production or commissioning line produces respectively commissions the intended set of products. Similarly, at one of more nodes of a supply chain, such as logistics centers, such reader devices may be integrated inline into identification and transport systems, e.g. conveyors, in order to automatically or semi-automatically (e.g. in the case of a handheld device) check and verify the authenticity of the products based on their markings, before shipping them to a next node in the supply chain. The same applies to a final node, i.e. to a recipient and/or end user of the products.

[0077] A seventh aspect of the present security solution is directed to a computer program

comprising instructions, which when executed on one or more processors of a reader device according to the sixth aspect cause the reader device to perform the method according to the fifth aspect of the present security solution.

[0078] The computer program may be particularly implemented in the form of a data carrier on which one or more programs for performing the method are stored. This may be advantageous, if the computer program product is meant to be traded as an individual product in individual product independent from the processor platform on which the one or more programs are to be executed. In another implementation, the computer program product is provided as a file on a data processing unit, particularly on a server, and can be downloaded via a data connection, e.g. the Internet or a dedicated data connection, such as a proprietary or local area network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0079] Further advantages, features and applications of the present security solution are provided in the following detailed description and the appended figures, wherein:

Fig. 1 schematically illustrates various composite security markings according to preferred embodiments of the present security solution;

Fig. 2 schematically illustrates a multi-part physical object according to a preferred embodiment of the present security solution, the object comprising a bottled consumable good and a related packaging, wherein the object is marked with a composite security marking according to the present security solution that comprises a PUF implemented on the bottle and a corresponding digital signature printed on the packaging;

Fig. 3 schematically illustrates another multi-part physical object according to a preferred embodiment of the present security solution, the object comprising as consumable goods a set of pharmaceutical tablets arranged in blister packs and a related packaging for the blister packs, wherein each of the tablets contains a UCD-based PUF and the packaging comprises a printing thereon which represents a set of the digital signatures corresponding to the PUFs;

Fig. 4 illustrates various different ways of deriving data representing a response generated by a UCD-based PUF in reaction to a corresponding challenge of a predetermined challenge-response authentication scheme, according to preferred embodiments of the present security solution;

Fig. 5 show a flow chart illustrating a basic method of marking a physical object with a composite security marking, according to preferred embodiments of the present security solution;

Fig. 6 schematically illustrates an apparatus for performing the method of Fig. 5, according to a preferred embodiment of the present security solution.

Figs. 7A and B show a flow chart illustrating a first embodiment of a method of reading with a reader device a marking comprising a PUF, such as a composite security marking of Fig. 1, according to a preferred embodiment of the present security solution;

Figs. 8A and 8B show a flow chart illustrating a second embodiment of a method of reading with a reader device a marking comprising a PUF, such as a composite security marking of Fig. 1, according to another preferred embodiment of the present security solution;

Fig. 9 schematically illustrates a reader device according to a preferred embodiment of the present security solution;

Fig. 10 a schematic overview of a preferred embodiment of the present security solution; and

Fig. 11 schematically an evolution of a set of two cross-connected blockchains along a supply chain for a product being marked with a composite security marking, according to preferred embodiments of the present security solution.

[0080] In the figures, identical reference signs are used for the same or mutually corresponding elements of the solution described herein.

DETAILED DESCRIPTION

A. Composite Security Marking

[0081] Fig. 1 shows six different variations (a) - (f) of a composite security marking 1 for a physical object, esp. a product, according to preferred embodiments of the present security solution. Each of these composite security markings 1 comprises a PUF 2 and a representation of a digital signature 3 that digitally signs a hash value derived from data representing a response received from the PUF in reaction to a challenge corresponding to a predetermined challenge-response authentication scheme. Accordingly, the PUF 2 and the digital signature 3 are related and correspond to each other. The digital signature 3 was created with the help of a private key of a public key/private key pair of an asymmetric cryptographic system. It can be read with the help of the corresponding public key of the asymmetric cryptographic system in order to verify the authenticity of the digital signature and thus the physical object marked with it.

[0082] Based on its nature, the PUF 2 can be considered unique (hence "unclonable") as is its response to the challenge. Accordingly, due to the collision resistant one-way nature of the cryptographic hash function also the hash value derived from the response is unique and thus pertains only to this exact PUF 2, as it is virtually impossible to have to identical hash values by applying said hash function to responses of different PUFs, and even more so, if the PUFs also

have to be present at the same time at a same location (spatial and time coincidence).

[0083] Therefore, such a composite security marking 1 is extremely difficult, if not impossible, to fake and can thus be used to protect physical objects, such as products and other goods, in particular against counterfeiting and tampering.

[0084] Fig. 1 (a) shows a first variant of such a composite security marking 1, wherein the PUF 2 is implemented as an area on the surface of the composite security marking 1 that contains a mix of UCDs already in its material or which has one or more additional layers containing a coating material or ink that contains such a mix of UCDs. The digital signature 3 is represented by a two-dimensional barcode, such as a QR code.

[0085] Fig. 1 (b) shows another variant, wherein the PUF 2 is implemented as a microstructure in the form of a random distribution of a large number (e.g. 10^6 or more) of light reflecting microscopic particles, which, when illuminated with coherent laser light of a specific wavelength as a challenge, create a characteristic speckle pattern by way of interference. The pattern can be detected with an optical sensor, such as a suitable digital camera, in order to generate data representing the response, e.g. as a digital image file.

[0086] Fig. 1 (c) shows yet another variant, wherein the PUF 2 is implemented by a hologram that contains hidden phase-coded or frequency-coded information. When illuminated with coherent laser light of a specific wavelength as a challenge the hologram generates a virtual holographic image from which the hidden information can be extracted as a response according to a challenge-responsive authentication scheme with the help of one or more optical sensors and suitable image processing algorithms. In this variant, the digital signature 3 is exemplarily implemented by way of an RFID chip, which is configured to emit a signal representing the digital signature 3, when activated.

[0087] Fig. 1 (d) shows yet another variant, wherein the PUF 2 is implemented by way of an image that is printed using ink containing a mix of different types of UCD's. Optionally, in addition hidden information may be steganographically embedded in the image. For example, there might be artificially created minimal specific color variations, which are invisible to the human eye, but which are used to encode such information and can be detected using suitable optical sensors in combination with respective analysis algorithms. In this variant, the digital signature 3 is exemplarily implemented as a numerical string.

[0088] Fig. 1 (e) shows yet another variant, wherein both the PUF 2 and the digital signature 3 are implemented as an integrated combination, by way of a bar code image that is printed using ink containing a mix of different types of UCD's. The barcode encodes the digital signature 3, while the ink material represents the PUF 2. This allows for an extremely compact implementation of the composite security marking 1.

[0089] Fig. 1 (f) shows yet another variant, wherein like in Fig. 1(e) both the PUF 2 and the digital signature 3 are implemented as an integrated combination, by way of a bar code image

that is printed using ink containing a mix of different types of UCD's. However, in distinction to Fig. 1 (e), the barcode does not encode the digital signature 3 itself. Instead, it encodes a pointer 4 that indicates, where the actual digital signature 3 can be accessed from a place that is not part of the composite security marking 1 itself. Preferably, this pointer 4 is a representation of an Internet address, e.g. of a server, from where the digital signature 3 can be downloaded or otherwise accessed. Again, this allows for an extremely complex implementation of the composite security marking 1, and in addition allows a central management, storage and provision of the respective digital signatures 3 of multiple composite security markings 1, e.g. those pertaining to a particular series of products of a given manufacturer.

[0090] Fig. 2 shows a multi-part physical object according to a preferred embodiment of the present security solution. The object comprises a consumable good 6, such as a liquid pharmaceutical, that is contained in a container, esp. a bottle 5, and a related packaging 7. A composite security marking 1 is split into two parts on different substrates. As a first part of the composite security marking 1, a PUF 2 is placed on the bottle 5. The type of the PUF 2 can be any type of PUF as described herein, in particular as described in connection with Fig. 1 above. The second part of the composite security marking 1 comprises a barcode representing the digital signature 3 corresponding to the PUF 2 and being printed on the packaging 7. As the PUF 2 and the digital signature 3 are interlinked as described above, any counterfeiting by way of replacing the packaging 7 or the bottle 5 can be detected by way of identifying a mismatch between the hash value that can be derived from the response received in reaction to a related challenge according to the predetermined challenge-response authentication scheme and the hash value that is contained in and cryptographically protected by the digital signature 3.

[0091] Fig. 3 shows another multi-part physical object according to a further preferred embodiment of the present security solution. Here, the products to be protected are pharmaceutical tablets (pills) 8 which are contained in a set of blister packs 9. Each of the tablets contains a mix of UCDs of a type which do not cause detrimental effects on a mammal, esp. a human body, when swallowed. The mix of UCDs may be the same for all tablets or, alternatively, even individual per tablet or a subset thereof. As in Fig. 2, a packaging 7 forms a second part of the physical object to be protected and bears the digital signature(s) 3 corresponding to the one or more PUFs 2 contained in the tablets 8. In this way, when the PUF 2 is an integral inseparable part of the consumable good itself, the level of security can be further enhanced in comparison to a situation according to Fig. 2, where only the container 5 for the consumable good is bearing the PUF 2.

[0092] Fig. 4 illustrates various different ways (a) - (c) of deriving data representing a response generated by a UCD-based PUF 2 in reaction to a corresponding challenge of a predetermined challenge-response authentication scheme. In particular, the challenge may comprise irradiation of the PUF 2 by electromagnetic radiation having particular properties, e.g. a certain wavelength range or spectrum, such as particular spectral components in the infrared or UV part of the electromagnetic spectrum.

[0093] Fig. 4 (a) shows a first variant, wherein a spectrum $I(\lambda)$ of an intensity I of light emitted by the PUF 2 in response to the challenge is detected as a function of the wavelength λ. In particular, selected wavelengths λ_1, λ_2, λ_3, ..., at which peaks of the spectrum $I(\lambda)$ occur, can be identified by way of spectrum analysis or even simply by use of adequate intensity thresholds. By way of example, and without limitation, this information can then be represented by a data string F, which in a simple form only represents the values of the respective wavelengths λ_1, λ_2, λ_3 etc.. In an enhanced version, also the corresponding intensity values I_1, I_2 and I_3 etc. for these wavelengths are included in F, as indicated on the right side of Fig. 4(a). Alternatively, or in addition, other characteristics of the spectrum $I(\lambda)$ can be identified and represented by F. The data string F may in particular be a binary number consisting of a series of bits. Furthermore, the data string F can be interpreted as a "spectral barcode" which represents genuine features of the spectrum $I(\lambda)$, in particular in its graphical representation as shown on the right side of Fig. 4(a). In this variant, the intensity values I are analog values, i.e. they can have any value that can be represented by the data string F.

[0094] Fig. 4 (b) shows another variant, which is similar to that of Fig. 4 (a) with the exception that the intensity values I are quantized and can take on only one of three possible values, which in this example are normed values "0", "1/2" and "1" of a suitable intensity unit. This variant can be advantageously used to create a particularly robust way of representing the spectrum by the data string F, because due to the quantization the resulting data string F is less sensitive to variations in the detected values I caused by imperfections of the measurement itself. The data strings F of the variants shown in Figs. 4(a) and 4(b) each form implementations of a spectral barcode.

[0095] Fig. 4 (c) shows yet another variant, wherein the intensity $I(t, \lambda)$ of luminescent light, preferably fluorescent light, emitted from a PUF as a response to the challenge is detected to as a function of the time t and wavelength λ. A characteristic lifetime $T = T(\lambda)$ is determined, which may for example correspond to the half-life period $T_{1/2}$ of the luminescent light of the wavelength λ. A corresponding data string F may again be formed as a representation of the response. In particular, the data string F may include the characteristic lifetimes $T_i(\lambda)$ and the related wavelengths λ_i, i =1, 2, ... of a set of different wavelengths, which are preferably those wavelengths where peaks of the spectrum $I(\lambda)$ are detected.

[0096] While for the sake of simple illustration, the above examples have been described using a one-dimensional data string F as a representation of the response, other forms of data representations, in particular also multi-dimensional forms such as matrices, are also possible.

6. Providing a physical object with a composite security marking

[0097] A method and an exemplary apparatus for providing a physical object with a composite security marking according to the present security solution, are illustrated in **Figs. 5 and 6.**

[0098] Specifically, **Fig. 5** is a flow chart illustrating a basic method of marking a physical object with a composite security marking. **Fig. 6** schematically illustrates an apparatus 17 for performing the method of Fig. 5, according to a preferred embodiment involving an additive manufacturing process (3-D printing). The apparatus 17 comprises a 3-D printer 12, a PUF-scanner 14, a processing device 15 and a barcode printer 16. Furthermore, the apparatus 17 it may further comprise a container 11 for a raw material and means (not drawn) for mixing UCDs provided from a supply 10 with a 3D printing raw material. Optionally, some or all of these components 10 to 16 may be integrated into a same device.

[0099] In a first step S5-1 of the method, a PUF 2 (optionally a plurality of different PUFs) is added to a physical object to be marked, which may for example and without limitation be one of the pharmaceutical products illustrated in Figs. 3 and 4, or a spare part, seeding material etc., as already discussed in the summary section above. In the case of the apparatus 17 of Fig. 6, the physical object will typically be a solid object that can be 3-D printed. In this case, step S5-1 may comprise adding one or more types of UCD (preferably a secret mix of UCDs) to the container 11 containing a raw material, e.g. in the form of a powder, suitable for 3-D printing. The UCD and the raw material are mixed, and then the resulting material mix is provided to the 3-D printer 12 as a 3-D printing material. With the help of the 3-D printer 12 a product 13, such as for example a medical device in the form of a mesh, is printed according to a product design specification delivered to the 3-D printer 12 by way of a respective design file. As the UCDs had been mixed into the raw material before printing, the resulting product 13 incorporates these UCDs, which together form one or more PUFs 2.

[0100] In a further step S5-2, the product 13 resulting from step S5-1 is exposed to a challenge C that is emitted by the PUF-scanner 14 in the form of electromagnetic radiation of a wavelength respectively wavelength range corresponding to the predetermined challenge-response authentication scheme pertaining to the PUF(s) 2 incorporated in the product 13. In a further step S5-3, which typically occurs substantially simultaneously with step S5-2, the PUF-scanner 14 detects a response R emitted by the PUF(s) 2 being incorporated in the product 13 in reaction to the challenge C. The response is then transformed into a data string F representing it, for example as described above in connection with Fig. 4. Particularly, and without limitation, the data string F may be a binary string, as illustrated. If there are two or more PUFs 2, the data string F may in particular represent the individual responses of all of these PUFs 2, which may optionally also be interpreted as a combined single response of a combined PUF comprising all of the individual PUFs.

[0101] In a further step S5-4, the data string F is provided to the processing device 15 as an input, which applies a predetermined cryptographic hash function H(...) to the data string F, in order to generate a hash value H = H(F) representing the response R. In a further step S5-5, with the help of the processing device 15 the resulting hash value H is digitally signed with a private key of a public/private key pair of an asymmetric cryptographic system, such as the well-known RSA scheme, in order to generate a digital signature 3 comprising the hash value H itself and a digitally signed version S[H(F)] thereof.

[0102] In a further step S5-6a, using the barcode printer 16, the digital signature 3 is printed to a surface of the product 13 in the form of a two-dimensional barcode, e.g. a QR-code or a DATAMATRIX code. As a consequence, the finished product 13 now comprises both the PUF(s) 2 and the corresponding digital signature (3) and thus a complete composite security marking 1 according to the present security solution.

[0103] In an alternative variant, a further step S5-6b is performed instead of step S5-6a. Step S5-6b is similar to step S5-6a, with the exception that instead of the digital signature 3 itself only a pointer 4 indicating where the digital signature 3 can be accessed, e.g. at a database or at an Internet server, is printed on the product 13. Before, simultaneously or after step S5-6b, a further step S5-7 is performed wherein the digital signature 3 obtained in step S5-5 is stored by the processing device over a data link to the location indicated by the pointer 4 for later access.

[0104] In both variants S5-6a and S5-6b, a representation of the digital signature 3 respectively of the pointer 4 may be added, instead or in addition to printing, in the form of an electronic representation, e.g. a RFID chip that is arranged to emit a signal carrying said representation upon receiving a respective trigger signal (cf. Fig. 1(c)).

C. Reading of a Marking comprising a PUF

[0105] The reading of a marking comprising a PUF, in particular of a composite security marking according to the first aspect of the present security solution, for example as shown and described in connection with Fig. 1, is now described in connection with corresponding **Figs. 7A to 9.**

[0106] Figs. 7A and 7B together show a flow chart (split in two parts connected via connector "A") illustrating a first preferred embodiment of a method of reading with a reader device a marking comprising a PUF, such as a composite security marking of Fig. 1. The method comprises, optionally, a first phase comprising steps S7-1 to S7-7, which serve for enhancing the security of a reader device itself that performs the method.

[0107] Step S7-1 is an access monitoring step, wherein sensor outputs are evaluated, in order to detect, as a security event, an attempt or actual act of physical intrusion into the reader device, or an attempt or actual act of locally or remotely accessing an internal control functionality, such as a processing device or communication device, of the reader device. If in a further step S7-2, it is determined that in step S7-1 a security event was detected (S7-2; yes), the method performs a security defense step S 7-5 as a final step, wherein an error message indicating the security event is output at a user interface and/or is sent over a communication link to an opposing side, such as a predetermined trust center. Furthermore, the reader device may be locked and/or the reader device or at least data stored therein may be self-destroyed in order to avoid unauthorized access to the data or any functionality of the reader device.

Otherwise (S7-2; no), the method proceeds to an information monitoring step S7-3.

[0108] In the information monitoring step S7-3 a signal is received over a communication link from a central authority of the security solution, such as a trust center providing a security server, and is evaluated in order to detect whether a security event is indicated by the information contained in the signal. If in a further step S7-4, it is determined that in step S7-3 a security event was indicated in the information (S7-4; yes), the method proceeds to and performs the security defense step S7-5 as a final step.

[0109] Otherwise (S7-4; no), the method proceeds to an authentication step S7-5.

[0110] In the authentication step S7-5 a user of the reader device is authenticated, e.g. via a suitable user interface, such as a keyboard for inputting a password or a fingerprint sensor etc.. If in a further step S7-7, it is determined that the authentication of step S7-6 failed (S7-7; no), the method returns to step as 7-1 or, alternatively, to the authentication step S7-6 (not drawn). Otherwise (S7-7; yes), the method proceeds to a second phase, wherein the marking is read and a reading result is output.

[0111] This second phase comprises a stimulation step S7-8, wherein a physical challenge according to a predetermined challenge-response-scheme corresponding to a PUF comprised in the marking is created and applied to the PUF, which might contain for example a mix of different UCDs.

[0112] Subsequently or simultaneously with the stimulation step S7-8, a detection step S7-9 is performed, wherein a response generated by the PUF in reaction to the physical challenge and according to the challenge-response authentication scheme is detected and a digital signal is generated that represents the response and which might for example take the form of or include a spectral barcode, as discussed above.

[0113] In a subsequent processing step S7-10 the digital signal is processed in order to generate a hash value of the response by application of a predetermined cryptographic hash function to the digital signal. Optionally, the processing step may further comprise digitally signing said hash value in order to provide a (first) digital signature thereof.

[0114] The processing step S7-10 is followed by an output step S7-14a, wherein a (first) reading result is output, for example on a user interface of the reader device or in a datastream or file provided at an electronic or optical interface of the reader device. The (first) reading result comprises data representing the hash value generated in the processing step and/or a representation of said (first) digital signature. Accordingly, this method can be used to read a marking comprising a PUF, in particular a composite security marking, as disclosed herein (e.g. in Fig. 1) and to output a corresponding reading result that is based on the response generated by the PUF. This reading result may be used for authentication purposes in the field (e.g. at various nodes along a supply chain of products being marked), or even initially at a fabrication or commissioning site, when a physical object is initially marked, in order

to verify the marking and in order to capture its response for further use, e.g. for storing it in a database for subsequent authentication purposes.

[0115] Figs. 8A and 8B together show a flow chart (split in two parts connected via connector "B") illustrating a second preferred embodiment of a method of reading with a reader device a marking comprising a PUF, such as a composite security marking of Fig. 1. Optionally, this method may comprise a similar first phase comprising steps S8-1 to S8-7 (which correspond to steps S7-1 to S7-7 of Fig. 7A) for enhancing the security of a reader device itself. Furthermore, the method comprises a stimulation step S8-8, a detection step S8-9, and a processing step S8-10, wherein these steps correspond to and may in particular be identical to steps S7-8 to S7-10 of Figs. 7A and 7B.

[0116] The method further comprises an acquisition step S8-11, wherein a first digital signature comprised in the composite security marking is acquired and a second digital signature pertaining to the marking is accessed. In particular, such access may be performed by acquiring from the composite security marking a pointer indicating a source where the second digital signature can be accessed, e.g. from a remote server. The second digital signature is read from said source and a matching flag is initialized (unset). The acquisition step S8-11 may be performed before, simultaneously, or after the processing step S8-10.

[0117] In a subsequent matching step S 8-12, the hash value signed by and comprised in the acquired first digital signature and a hash value generated in the processing step S8-10 are compared. If the two hash values match (S8-12; yes), the matching flag is set (step S8-13), otherwise (S8-12; no) the matching flag is not set. Of course, using such a matching flag is only one of many different possible implementations of determining and communicating whether or not the two hash values match.

[0118] The method further comprises an output step S8-14b, wherein various reading results are output, for example on a user interface of the reader device or in a data stream or file provided at an electronic or optical interface of the reader device. In particular, the reading results include a (first) reading result which comprises data representing the hash value generated in the processing step and/or a representation of said (first) digital signature. Other reading results may comprise a representation of the acquired first digital signature, a representation, e.g. as a barcode, of the read second digital signature, and/or a matching output indicating (i) a match, if the matching flag is set, and (ii) a mismatch otherwise. Accordingly, also this method can be used to read a marking comprising a PUF, particularly a composite security marking, as disclosed herein (e.g. in Fig. 1) and to output a corresponding reading result that is based on the response generated by the PUF. Again, this reading result may particularly be used for authentication purposes in the field (e.g. at various nodes along a supply chain of products being marked).

[0119] The method further comprises a storage step S8-15, which is preferably performed simultaneously or after the output step S8-14b. In the storage step S8-15 the first reading result comprising data representing the hash value generated in the processing step is stored

into a block of a first blockchain and the second reading result obtained in the acquisition step is stored into a block of a second, separate blockchain. Furthermore, related cross-blockchain pointers connecting the two blockchains are stored into each of the two blockchains to indicate the blocks in each of the blockchains, which correspond to each other in this sense, that they contain data created and stored at the same reading event. In particular, the second blockchain might be related to supply-chain information, such as time, location and user identification of the current reading event. The first blockchain, on the other hand, is used for tracking the authentication information, in particular, whether or not at the current reading event the physical object bearing the marking has been successfully authenticated as being original (i.e. not counterfeited or tampered with).

[0120] Furthermore, the method may comprise a communication step S8-16, wherein the data output in the output step, including the matching output, and optionally also a timestamp and/or a current location of the reading event respectively the reader device (each of which can be considered security-related information) is sent over a communication link to a predetermined central server, which may for example form a part of a trust center.

[0121] Fig. 9 schematically illustrates a reader device 20, according to a preferred embodiment of the present invention. In particular, the reader device may be adapted to perform the method of Figs. 7A and 7B and/or Figs. 8A and 8B. By way of example, and without limitation, the reader device 20 may form a component of or be used in connection with a manufacturing or commission line, which is illustrated in Fig. 9 by way of a conveyor 31 on which physical objects 32, i.e. products, each bearing a composite security marking as disclosed herein (e.g. in Fig. 1) are transported to and from the reader device 20.

[0122] The reader device 20 may comprise various different components 21 to 30, which are communicatively interconnected by a data bus 33 or any other suitable communication technology. In particular, the reader device 20 comprises a stimulator 21 adapted to generate and apply to a composite security marking 1 on the product 32 passing by on the conveyor 31 a stimulation according to a predetermined challenge-response authentication scheme, and a corresponding PUF-detector 22 adapted to detect the response emitted by the PUF of the marking in reaction to the stimulation. For example, if the PUF comprises a mix of different UCDs, the stimulator 21 may be adapted to admit a suitable electromagnetic radiation in order to stimulate the UCD's in the PUF to re-emit electromagnetic radiation being characteristic for the specific PUF of the marking. Accordingly, in such case the PUF-detector is adapted to detect such a re-emitted radiation and spectrally analyze it in order to derive a digital signal, e.g. in the form of a spectral barcode, that represents the response and which can be further processed.

[0123] Furthermore, the reader device 20 may comprise an acquisition device 23 that is adapted to acquire a first digital signature comprised in the composite security marking. In particular, the acquisition device 23 may be adapted to perform a step similar to step S8-11 of Fig. 8B.

[0124] In addition, the reader device 20 may comprise a communication device 24 that is adapted to communicate with an opposing side 34, for example a central security server of a trust center, via a communication link. Particularly, the communication link may be implemented as a wireless link, in which case the communication device would typically comprise or be connected to an antenna 24a, or the link may be implemented by way of the cable, such as electrical or optical cable, as a non-wireless communication link 24b. Particularly, the reader device 20 may be configured to send reading results to be output in the output step (as in step 8-14b of Fig. 8B, for example) over the communication link in order to inform the opposing side 34 of the reading results and/or other information, such as security-related information (e.g. the occurrence of a security event at the reader device 20).

[0125] To further increase security, the reader device 20 may also comprise an authentication device 25 being adapted to authenticate a user of the reader device 20, before permitting access to it and/or its further use (such as in steps S8-6 and S8-7 of Fig. 8A).

[0126] The reader device 20 may further comprise a security device 26 comprising one or more sensors for detecting a security event, such as an attempt or actual act of physical intrusion into the reader device 20, or an attempt or actual act of locally or remotely accessing without authorization an internal control functionality of the reader device 20. Preferably, the security device 26 interacts with or further comprises a security defense arrangement 27 to protect the reader device 20 in case a security event was detected. Particularly, the security defense arrangement 27 may be adapted to perform a step similar to step S7-5 of Fig. 7A or to step S8-5 of Fig. 8A. For example, the security defense arrangement 27 may be configured to lock a user interface of the reader device 20 in case a security event is detected or to activate a self-destruction of a security chip contained in the reader device 20, in order to protect data stored therein, including for example a private cryptographic key or other security-relevant data such as authentication data. In addition to or instead of the security device 26, the reader device 20 may comprise a monitoring device 28, that is configured to detect a security event indicated in information contained in a signal received from the opposing side 34 over said communication link. For example, in case such opposing side 34, e.g. a trust center, learns about a broader attempt to attack the security and integrity of reader devices 20 being distributed in the field, e.g. along a given supply chain, such signal may be used to proactively trigger a blocking (at least temporarily) of any further use of the reader devices 20 in the field in order to prevent tampering with the reader devices 20 by such attacks.

[0127] Furthermore, the reader device 20 comprises a processing device 29 that is particularly adapted, e.g. by a respective software program running on it, to process the digital signal generated by the PUF-detector in order to generate a hash value of the response of the PUF by application of a predetermined cryptographic hash function to the digital signal (cf. steps S7-10 of Fig. 7B and step S8-10 of Fig. 8B). In some implementations, further functionality of the reader device 20 that involves data processing or control may be additionally implemented by the processing device 29. Accordingly, all or part of any processing functionality of the other components 21 to 28 and 30 of the reader device 20 may be incorporated into the processing device 29 instead of being implemented in separate components.

[0128] The reader device may also comprise a blockchain storing device that is adapted to store data in one or more blockchains, to which the reader device 20 is connectable via said communication link. In particular, said data may correspond to the reading results generated when the reader device is used for reading a marking comprising a PUF. While the blockchain storing device may be implemented as a separate component or module of the reader device 20, it is preferably included in the processing device 29, as in Fig. 9.

[0129] An output generator 30 forms a further component of the reader device 20. It is configured to output, e.g. on a user interface or on an electrical or optical interface, data representing the generated hash value as a first reading result, a representation of acquired digital signatures, such as the first digital signature and the second digital signature discussed above (cf. step S8-14b of Fig. 8B) and optionally, a matching output indicating whether or not the hash values resulting from the processing step (cf. step S8-10 of Fig. 8B) and the acquisition step (cf. step S8-11 of Fig. 8B) match (cf. step S8-12 of Fig. 8B).

D. Overall Security Solution

[0130] Figures 10 and 11 illustrate further preferred aspects of the overall security solution that is based on the use of markings comprising a PUF and on one or more reader devices, as discussed above. In particular, **Fig. 10** shows a schematic overview of a basic embodiment of a security system 14 based on the present security solution that allows for verifying, at a recipient B participating in a supply chain, whether a product being marked by a composite security marking 1 (e.g. per Fig. 1) is original and was in fact provided by the presumed original manufacturer A positioned upstream in the supply chain.

[0131] To that purpose, manufacturer A is equipped with an apparatus for applying a composite security marking 1 to the products 32 being subsequently shipped along the supply chain. For example, such apparatus may be an apparatus similar to the apparatus shown in Fig 6. Alternatively, manufacturer A may be equipped with a reader device 20, such as the one shown in Fig. 9, and use a separate apparatus for applying a corresponding composite security marking 1 carrying information read by the reader device 20, including a (first) digital signature comprising a hash value being derived from reading the PUF in the composite security marking 1. Accordingly, the apparatus 17 respectively 20 is configured to perform the corresponding method of Fig. 5 respectively of Figs. 7A and 7B. In addition, the apparatus 17 or 20 is equipped to generate a public/private key pair of an asymmetric cryptography system, store the private key (secure key, SK) in a secured storage space of the apparatus 17 respectively 20 and forward the public key (PUK) along with the first digital signature and optionally further security-related information, such as the time and/or location of the generation of the first digital signature, to a central security server 34 located in a trust center that is entertained by a trusted third party. Accordingly, the trust center plays the role of a registration authority, where a particular public keys of one or more apparatus 17 and reader devices 20 are registered and stored. Preferably, any communication to and from the trust

center is protected by encryption, in particular to prevent "man-in-the-middle attacks".

[0132] In order to increase the available security level, the public key may be provided to a certification authority of a public key infrastructure (PKI), particularly to a related certification authority server 42, where the public key is certified and included into a cryptographic certificate that is made available to manufacturer A and a validation authority (server) 41. Now, any further node in the supply chain being equipped with a reader device 20 as described herein, such as recipient B, can request the certificate from the validation authority 41 to use it for examining the marked product allegedly originating from manufacturer A for its authenticity. To that purpose, the reader device 20 at recipient B runs the method of Figs. 8A and 8B and thereby detects the PUF on the composite security marking 1 of the product 32 and reads the first digital signature contained therein including the hash value that is to be compared to the hash value derived from the detected response of the PUF. If both hash values match, this confirms that manufacturer A was in fact the originator of the product 32, otherwise that the product or its marking have been counterfeited or otherwise tampered with.

[0133] The result of this comparison, i.e. the matching result and optionally further security-related information, such as the time and location of the examination and/or the identity of a user of the reader device 20 carrying through the examination, or forwarded to and stored on the central security server 34 of the trust center. This allows for a central monitoring of the supply chain and early identification of any counterfeiting or tampering issues occurring along the supply chain. The central security server 34 may further be configured to generate or consolidate and make available via a data interface API track and trace data reflecting the processing of the product 32 along the supply chain based on the matching results and security-related information provided by any reader devices 20 being involved in the supply chain.

[0134] Fig. 11 refers to a further preferred embodiment of the present security solution, particularly of a security system 40, wherein blockchain technology is used in order to safely store and make available authentication data being generated along the supply chain. Specifically, Fig. 11 schematically illustrates an evolution of a set of two cross-connected blockchains in parallel to a supply chain for a product 32 being marked with a composite security marking 1, according to preferred embodiments of the present security solution. Particularly, the embodiments of Fig. 10 and Fig. 11 may be combined within a single solution.

[0135] The solution of Fig. 11 comprises a first blockchain BC-PUF that is configured to safely store and make available authentication information, in particular hash values derived from detecting PUFs contained in composite security markings 1 of related products 32, as described herein. In addition, a second blockchain BC-SCM is provided, which is configured to safely store and make available supply-chain information, such as serial numbers of the products 32, dates and locations of readings of the composite security markings 1 of the products 32 etc.. Particularly, such supply-chain data may be stored in the second blockchain BC-SCM in the form of or in addition to related hash values being generated from such data by application of a suitable hash function. The two blockchains BC-PUF and BC-SCM, which are

both configured to track the motion of the products 32 along the supply chain, have their related blocks, i.e. the blocks containing data pertaining to the same checkpoint along the supply chain, linked by cross-blockchain pointers, thus providing references from and to corresponding blocks.

[0136] At a first node of the supply chain, which is owned by a manufacturer A of a product 32, this product 32 is marked with a composite security marking 1, as described herein, e.g. of the kind shown in Fig. 1. Again, an apparatus 17 or a reader device 20, as described above with reference to Fig. 6 respectively Fig. 9, may be used for this purpose. In the course of this marking process, the composite security marking 1 is detected by the apparatus 17 respectively 20 and a respective hash values generated. Optionally, this hash value is confirmed by comparing it to a corresponding hash value provided by the first digital signature also contained in the composite security marking 1, and then it is stored in a first block of the blockchain BC-PUF as an initial PUF hash value as part of a first stored transaction #1 originated by manufacturer A.

[0137] The composite security marking 1 of the product 32 further comprises a second digital signature that includes a second hash value being derived from supply-chain related data pertaining to manufacturer A. This second hash value is read from the composite security marking 1, using apparatus 17 respectively reader device 20, and stored to a first block of the second supply chain BC-SCM as part of a first transaction #1 originated by manufacturer A, optionally along with further supply-chain related data. Both of these two first blocks contain data corresponding to the initial step of the supply chain being owned by manufacturer A and accordingly in each of the two blocks a cross-blockchain pointer to the respective corresponding block in the other blockchain is added, in order to allow for cross-referencing.

[0138] In a next step along the supply chain, product 32 reaches a second, intermediate node C, which might for example be owned by logistics company being responsible for the further transportation of the product along the supply chain. Node C is equipped with a further reader device 20 and thus performs an examination of the product 32 by running the method of Figs. 8A and 8B on said reader device 20 in relation to the composite security marking 1 of product 32. If this examination confirms manufacturer A as the originator of the product 32, a respective transaction #2 confirming the positive examination is stored into a second block of the first blockchain BC-PUF. Otherwise, said stored transaction #2 indicates a negative result of the examination, thus indicating a fraud in relation to product 32 respectively its composite security marking 1. In addition, an alarm or error message may be output by the output generator 30, e.g. on a user interface, of the reader device 20, or an alarm/error message might be sent to the central trust center 34 via communication link 24a or 24b in order to indicate said negative result.

[0139] The second block is cross-linked to the previous, i.e. first, block of said blockchain by addition of the block hash of said previous block. This entry into the first blockchain BC-PUF confirms that the product 32 was examined at node C with the respective result. The initial PUF hash value remains available via the cross-link to the first block. Similarly, as in the previous

node, supply chain information is generated from the second digital signature of the composite security marking 1 and further data related to the node and stored in the second blockchain BC-SCM as a transaction #2. Also in this second supply chain BC-SCM, the second block is cross-linked to the previous first block by storing a block hash of said previous block in the second block. Again, a cross-blockchain pointer is added in each of the second blocks to allow for cross-referencing between them.

[0140] In a next step along the supply chain, product 32 reaches a third, intermediate node d, which might for example be a remote logistic station that is not equipped with a reader device 20 but instead only with a conventional scanner that is only capable of reading the second digital signature comprised in the composite security marking 1 of product 32. Unlike in the previous nodes, at node d only supply chain related data is written to a third block of the second supply chain BC-SCM as a transaction #3, similarly as in node C. However, no data is stored in the first supply chain BC-PUF, as the scanner is not capable of reading the PUF of the composite security marking 1 and generate related data.

[0141] Finally, in a fourth step along the supply chain, product 32 reaches node B, which might for example be a final destination or a local retailer of the product 32. At this node B, a similar procedure is performed using another reader device 20, as at previous node C and accordingly, similar entries are added to respective further blocks of both blockchains PC-PUF and BC-SCM.

[0142] The two blockchains serve as a safe public ledger of all of said transactions which have ever occurred and have been stored since the initiation of said blockchains. Furthermore, the blockchains provide an extremely high integrity level as they cannot be manipulated (in practice) and thus their use further enhances the security of the overall security solution presented herein. In particular, the data stored in the two block chains can be used to examine both whether manufacturer A was in fact the originator of product 32 and whether the supply chain was as expected. This examination can be made at each node A, C, B along the supply chain that is equipped with a reader device 20 and thus can examine the composite security marking 1 of the product 32 and access the data stored in the two blockchains.

[0143] While above at least one exemplary embodiment of the present security solution has been described, it has to be noted that a great number of variation thereto exists. Furthermore, it is appreciated that the described exemplary embodiments only illustrate non-limiting examples of how the present security solution can be implemented and that it is not intended to limit the scope, the application or the configuration of the herein-described apparatus' and methods. Rather, the preceding description will provide the person skilled in the art with constructions for implementing at least one exemplary embodiment of the solution, wherein it has to be understood that various changes of functionality and the device of the elements of the exemplary embodiment can be made, without deviating from the subject-matter defined by the appended claims and their legal equivalents.

LIST OF REFERENCE SIGNS

[0144]

1 Composite security marking

2 Physical unclonable function, PUF

3 Digital signature corresponding to PUF

4 Pointer indicating where digital signature can be accessed

5 Bottle containing consumable good

6 Consumable good, in particular liquid pharmaceutical substance

7 Packaging

8 Pharmaceutical tablet, pill

9 Blister pack

10 Supply of mix of different UCDs

11 Container with raw material for 3-D printing

12 Additive manufacturing device, 3-D printer

13 3-D printed physical object/product

14 PUF-Scanner

15 Processing device

16 Barcode printer

17 Apparatus for providing a composite security marking to an object

20 Reader device

21 Stimulator

22

PUF-Detector

23
Acquisition device

24
Communication device

24a
Antenna

24b
non-wireless communication link

25
Authentication device

26
Security device

27
Security defense arrangement

28
Monitoring device

29
Processing device

30
Output generator

31
Conveyor of a production line

32
Marked physical objects (products)

33
Bus

34
Central security server, trust center

40
Security system

41
Validation Authority server

42
Certification Authority server

C
Challenge according to challenge-response authentication scheme

R
Response according to challenge-response authentication scheme

F
Data(string) representing response by PUF to challenge

H(F)
Cryptographic hash function applied to F, yielding hash value H= H(F)

S[H(F)]
: Digital signature of hash value H

λ,
: Wavelengths

λ_i
: Wavelength, at which a peak of the light intensity I occurs in the response

R I
: Light intensity

I_i
: Light intensity at wavelength λ_i

REFERENCES CITED IN THE DESCRIPTION

Cited references

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO2007031908A2 [0010]
- EP2999156B1 [0011]
- EP2911335A1 [0012]

Non-patent literature cited in the description

- **VIRGINIA TECH**Background on Physical Unclonable Functions (PUFs)Department of Electrical and Computer Engineering, 2011, [0005]
- **PA WAN KUMAR et al.**NANOSCALE, 2016, vol. 8, 302040-336414297-14340 [0009]
- **DAN JIANG et al.**Anti-counterfeiting using phosphor PUF2ND INTERNATIONAL

CONFERENCE ON IEEE in PISCATAWAY, NJ, USA, 2008, [0013]

Patentkrav

1. Fremgangsmåde til læsning med en læseindretning af en markering omfattende en fysisk ikke-klonbar funktion, PUF, omfattende følgende trin:

et stimuleringstrin, hvor en fysisk udfordring i overensstemmelse med et forudbestemt udfordringssvarautentificeringssystem svarende til PUF'en genereres og anvendes for en PUF;

et detekteringstrin, hvor et svar genereret af PUF'en i overensstemmelse med udfordringssvarautentificeringssystemet som reaktion på udfordringen detekteres, og et digitalt signal, som repræsenterer svaret, genereres;

et bearbejdningstrin, hvor det digitale signal bearbejdes for at generere en hash-værdi for svaret ved anvendelse af en forudbestemt kryptografisk hash-funktion på det digitale signal, og

et udlæsningstrin, hvor data, som repræsenterer den genererede hash-værdi som et første læseresultat, udlæses, og hvor udlæsningstrinnet yderligere omfatter udlæsning af mindst en del af et læseresultat i form af en endimensionel eller en flerdimensionel stregkode,

hvor detektering af svaret i detekteringstrinnet omfatter detektering af mindst en egenskab af elektromagnetisk stråling emitteret af PUF'en som et svar som reaktion på udfordringen, detektering af en karakteristisk levetid af en luminescenseffekt, som finder sted i svaret som en egenskab af elektromagnetisk stråling emitteret af PUF'en, og det digitale signal genereres, således at det repræsenterer dette svar.

2. Fremgangsmåden ifølge krav 1, hvor det digitale signal genereres i bearbejdningstrinnet, således at det repræsenterer mindst en PUF-specifik særlig egenskab af svaret, som er, i det mindste i alt væsentligt, invariant under variationer af omgivelsesbetingelserne, ved hvilke svaret detekteres.

3. Fremgangsmåden ifølge et eller flere af de foregående krav, hvor:

detektering af svaret i detekteringstrinnet omfatter detektering af et spektrum af den emitterede stråling som en egenskab af elektromagnetisk stråling emitteret af PUF'en; og

bearbejdning af det digitale signal i bearbejdningstrinnet omfatter bestemmelse ud fra det digitale signal af en eller flere af følgende:

- positionen af et eller flere karakteristiske kendetegn inden for spektret;
- et eller flere statistiske mål som kendetegner spektret;
- en eller flere kvantiserede spektralværdier af spektret;
- en spektral stregkode som repræsenterer et kontinuerligt eller et kvantiseret interval af tilladte spektralværdier, som optræder i spektret.

4. Fremgangsmåden ifølge et eller flere af de foregående krav, yderligere omfattende:

et registreringstrin, hvor en kombineret sikkerhedsmarkering omfattende en PUF og en tilsvarende første digital signatur eller en pointer, som indikerer en kilde, hvor en sådan første digital signatur kan tilgås, læses, og nævnte første digitale signatur registreres fra henholdsvis markeringen eller kilden indikeret af nævnte pointer; og

i udlæsningstrinnet bliver en repræsentation af den registrerede første digitale signatur, og/eller en matchende udlæsning, som indikerer, om en hash-værdi, i overensstemmelse med mindst et forudbestemt matchende kriterie, tilvejebragt og underskrevet af den registrerede første digitale signatur matcher hash-værdien genereret fra svaret på udfordringen, udlæst.

5. Fremgangsmåden ifølge krav 4, hvor registreringstrinnet yderligere omfatter registrering ud fra den kombinerede sikkerhedsmarkering af en anden digital signatur eller en pointer, som indikerer en kilde, hvor en bestemt anden digital signatur vedrørende markeringen kan tilgås; og

udlæsningstrinnet yderligere omfatter udlæsning af en repræsentation af den registrerede anden digitale signatur som et andet læseresultat.

6. Fremgangsmåden ifølge et eller flere af de foregående krav, yderligere omfattende et autentificeringstrin, hvor en bruger autentificeres, før han eller hun får lov til yderligere at betjene læseindretningen i tilfælde af en succesfuld autentificering.

7. Fremgangsmåden ifølge et eller flere af de foregående krav, yderligere omfattende et kommunikationstrin, hvor et læseresultat kommunikeres over et kommunikationslink til en modsat side.

8. Fremgangsmåden ifølge krav 7, hvor kommunikationstrinnet yderligere omfatter indhentning og afsendelse af sikkerhedsrelateret information til en forudbestemt modsat side over kommunikationslinket.

9. Fremgangsmåden ifølge krav 7 eller 8, yderligere omfattende et informations-overvågningstrin, hvor en sikkerhedshændelse detekteres i information indeholdt i et signal modtaget fra den modsatte side over kommunikationslinket.

10. Fremgangsmåden ifølge et eller flere af de foregående krav, yderligere omfattende et adgangsovervågningstrin, hvor en eller flere af følgende detekteres ved hjælp af en eller flere sensorer som en sikkerhedshændelse:

- et forsøg på eller en faktisk handling til fysisk indtrængen i læseindretningen;
- et forsøg på eller en faktisk handling til lokalt eller på afstand at få adgang til en intern styrefunktionalitet af læseindretningen, hvor sådan adgang ikke er tilgængelig for en bruger af indretningen under den normale drift.

11. Fremgangsmåden ifølge krav 9 eller 10, yderligere omfattende et sikkerhedsbeskyttelsestrin, hvor en eller flere af følgende sikkerhedsforanstaltninger udføres som reaktion på detektering af en sikkerhedshændelse:

- blokering af læseindretningen for at begrænse eller forhindre yderligere anvendelse deraf;
- selvdestruktion af mindst en funktionel del af læseindretningen eller destruktion af data lagret deri for at forhindre yderligere anvendelse deraf eller adgang af en bruger.
- udlæsning af en fejlmeddelelse.

12. Fremgangsmåden ifølge et eller flere af de foregående krav, hvor udlæsningstrinnet omfatter digital signering af data indeholdende den genererede

hash-værdi og udlæsning af den resulterende digitale signatur som det første læseresultat.

13. Fremgangsmåden ifølge et eller flere af de foregående krav, yderligere omfattende et lagringstrin, hvor et læseresultat, som udlæses i udlæsningstrinnet, lagres i en blok af en blockchain.

14. Fremgangsmåden ifølge krav 5 og 13, hvor lagringstrinnet omfatter:

lagring af et først læseresultat omfattende data som repræsenterer hash-værdien genereret i bearbejdningstrinnet til en blok af en første blockchain; og

lagring af det andet læseresultat opnået i registreringstrinnet ifølge krav 5 til en blok af en anden blockchain som er separat fra den første blockchain.

15. Fremgangsmåden ifølge krav 14, hvor lagringstrinnet yderligere omfatter:

ved lagring af det første læseresultat i en blok af den første blockchain, at inkludere en cross-blockchain pointer, som logisk afbilder blokken af den første blockchain til en tilsvarende blok af den anden blockchain til blokken af den første blockchain; og

ved lagring af det andet læseresultat i en blok af den anden blockchain, at inkludere en cross-blockchain pointer, som logisk afbilder blokken af den anden blockchain til en tilsvarende blok af den første blockchain til blokken af den anden blockchain.

16. Læseindretning til læsning af en markering omfattende en fysisk ikke-klonbar funktion, PUF, hvor læseindretningen er indrettet til at udføre fremgangsmåden ifølge et eller flere af de foregående krav.

17. Læseindretningen ifølge krav 16, omfattende:

en stimulator konfigureret til at udføre stimuleringstrinnet;

en PUF-detektor konfigureret til at udføre detekteringstrinnet;

en bearbejdningsindretning konfigureret til at udføre bearbejdningstrinnet; og

en udlæsningsgenerator konfigureret til at udføre udlæsningstrinnet.

18. Læseindretningen ifølge krav 17, yderligere omfattende en eller flere af følgende:

- en registreringsindretning konfigureret til at udføre registreringstrinnet ifølge krav 4 eller 5;
- en autentificeringsindretning konfigureret til at udføre autentificeringstrinnet ifølge krav 6;
- en kommunikationsindretning konfigureret til at udføre kommunikationstrinnet ifølge krav 7 eller 8;
- en overvågningsindretning konfigureret til at udføre informationsovervågningstrinnet ifølge krav 9;
- en sikkerhedsindretning omfattende mindst en sensor og konfigureret til at udføre adgangsovervågningstrinnet ifølge krav 10;
- en sikkerhedsbeskyttelsesanordning konfigureret til at udføre sikkerhedsbeskyttelsestrinnet ifølge krav 11;
- en blockchain-lagringsindretning konfigureret til at udføre lagringstrinnet ifølge et hvilket som helst af kravene 13 til 15.

19. Computerprogram omfattende instruktioner, som, når de eksekveres på en eller flere processorer af en læseindretning ifølge et eller flere af kravene 16 til 18, får læseindretningen til at udføre fremgangsmåden ifølge et hvilket som helst af kravene 1 til 15.

DRAWINGS

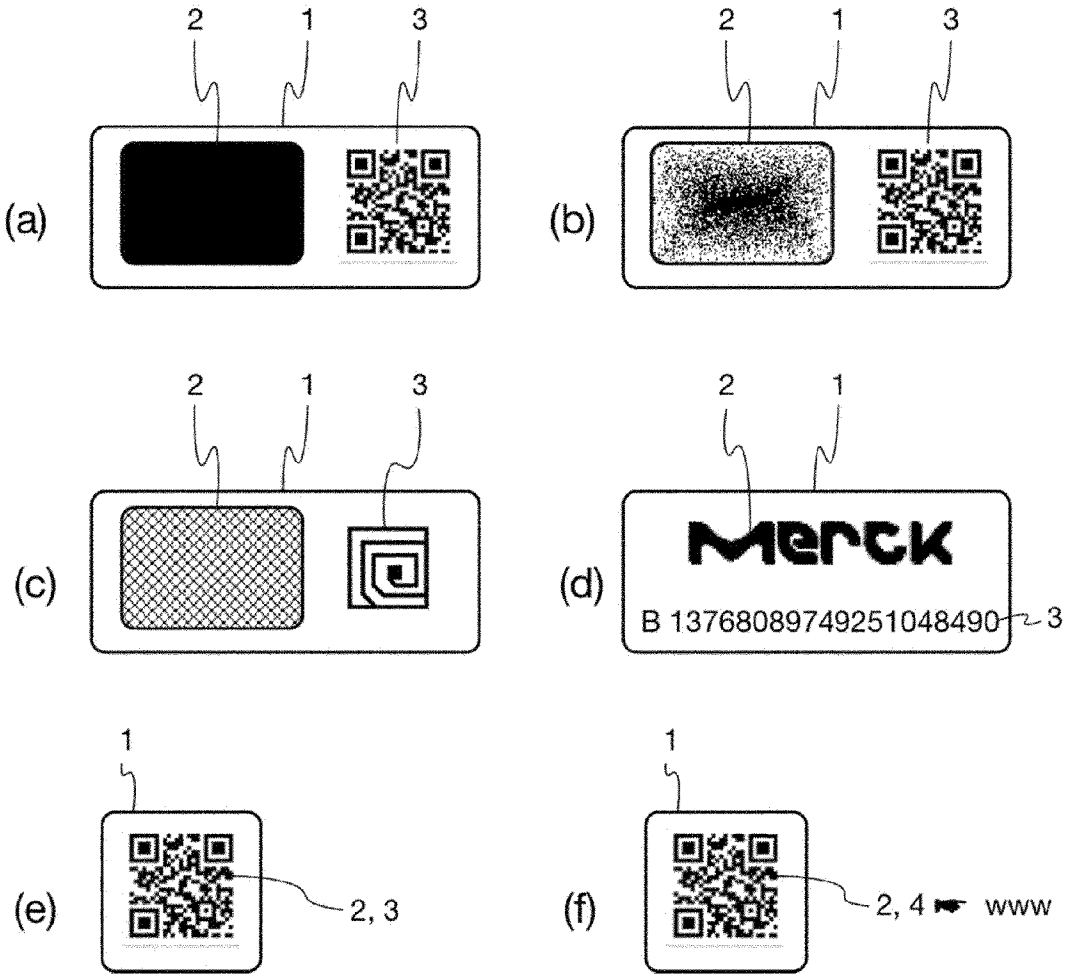

Fig. 1

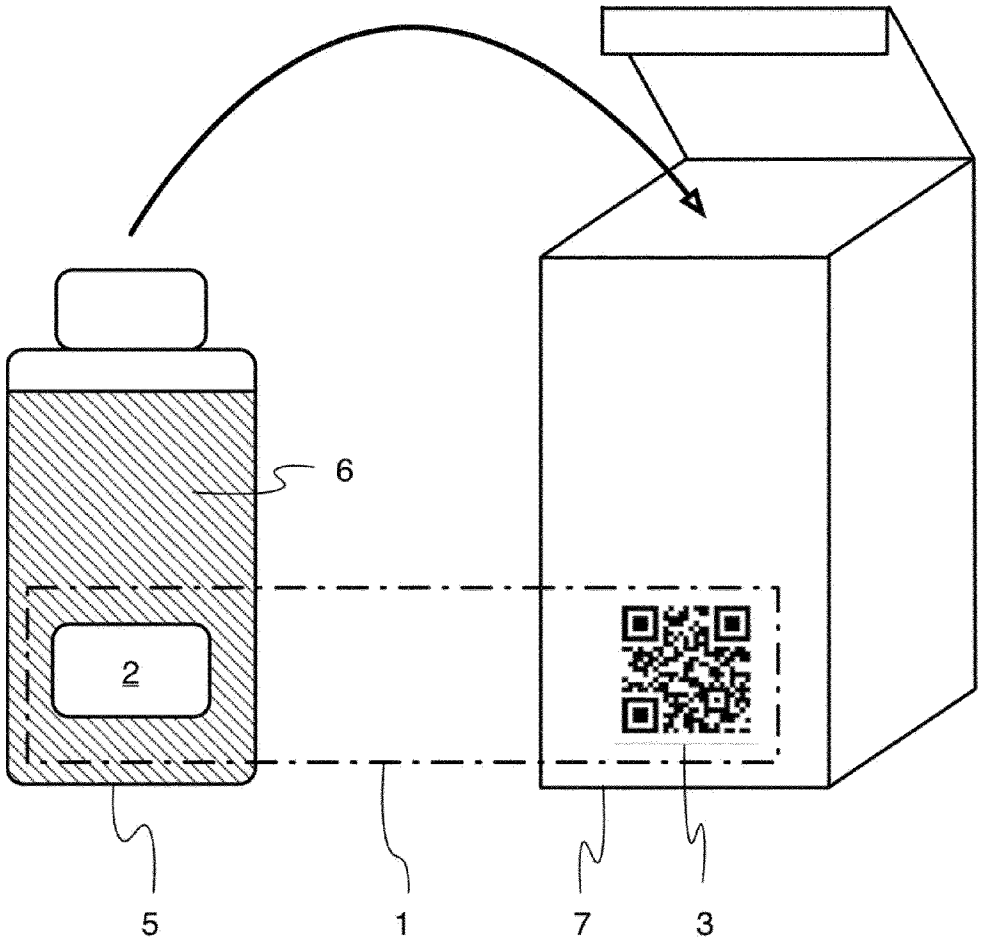

Fig. 2

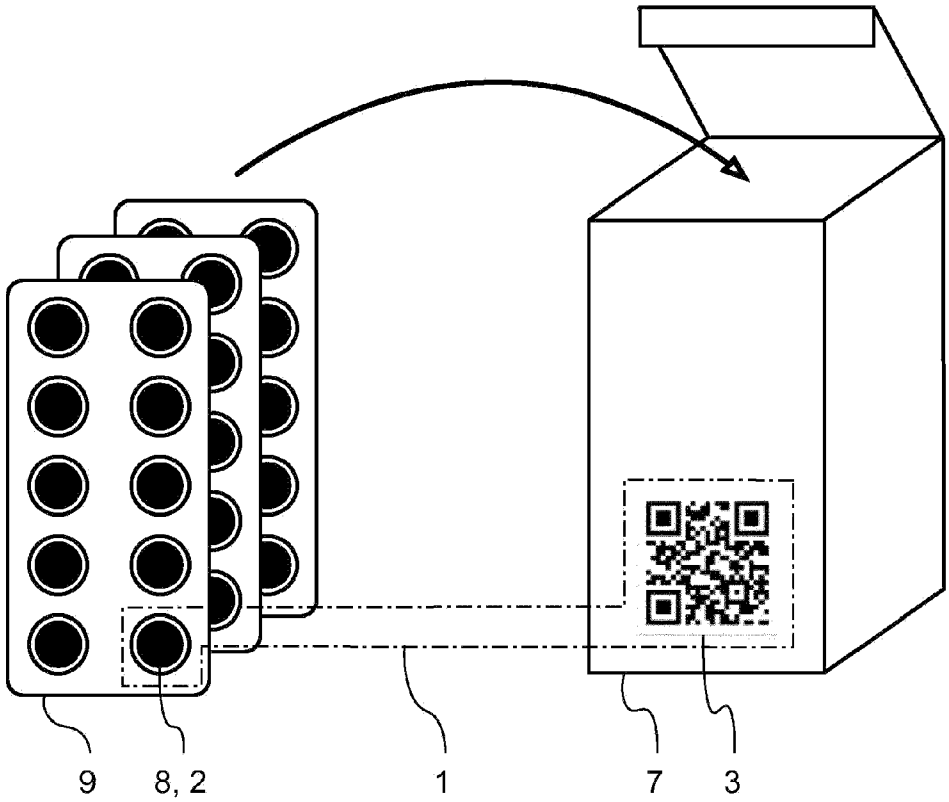

Fig. 3

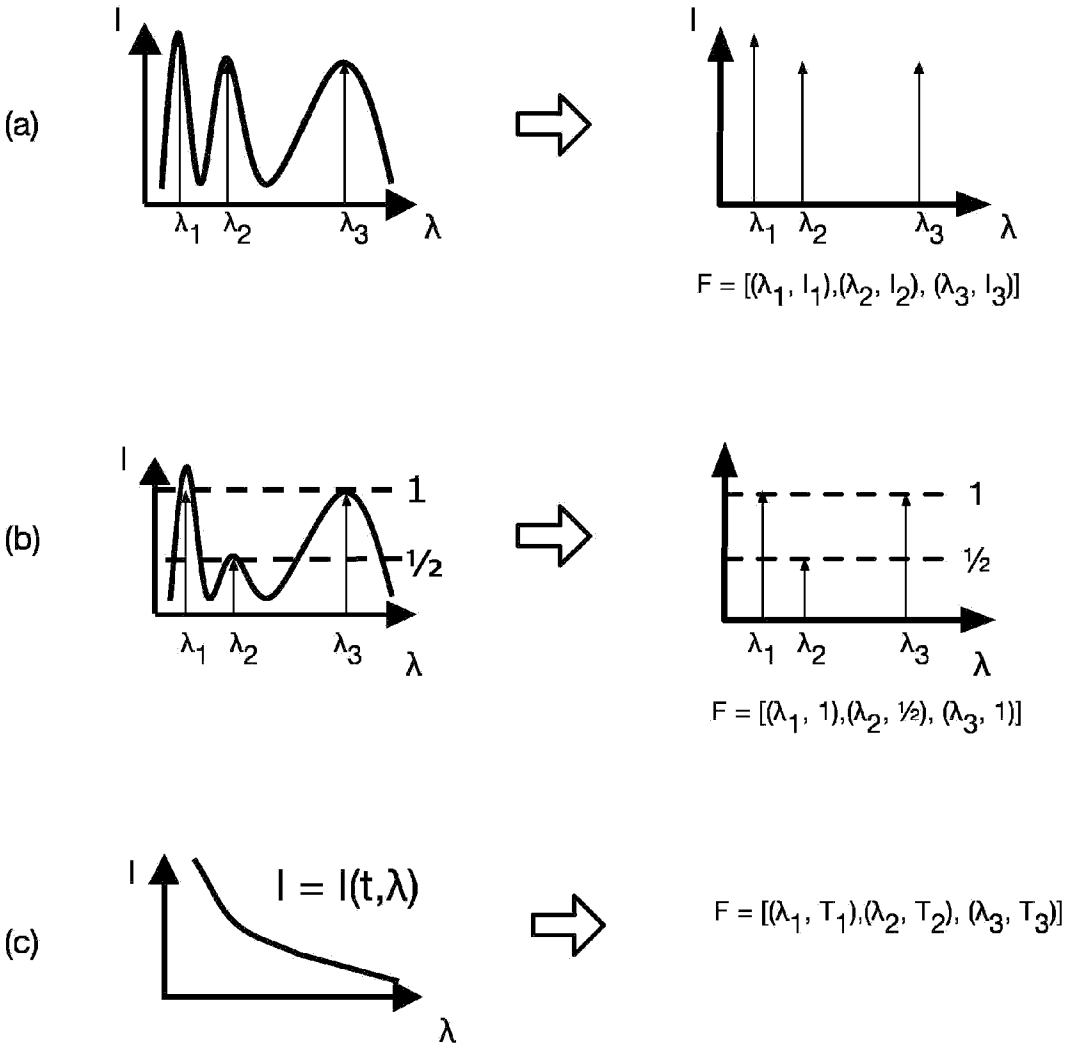
(a)
I
λ1 λ2 λ3 λ
I
λ1 λ2 λ3 λ
F = [(λ1, I1),(λ2, I2), (λ3, I3)]
(b)
I
1
½
λ1 λ2 λ3 λ
1
½
λ1 λ2 λ3 λ
F = [(λ1, 1),(λ2, ½), (λ3, 1)]
(c)
I
I = I(t,λ)
λ
F = [(λ1, T1),(λ2, T2), (λ3, T3)]

Fig. 4

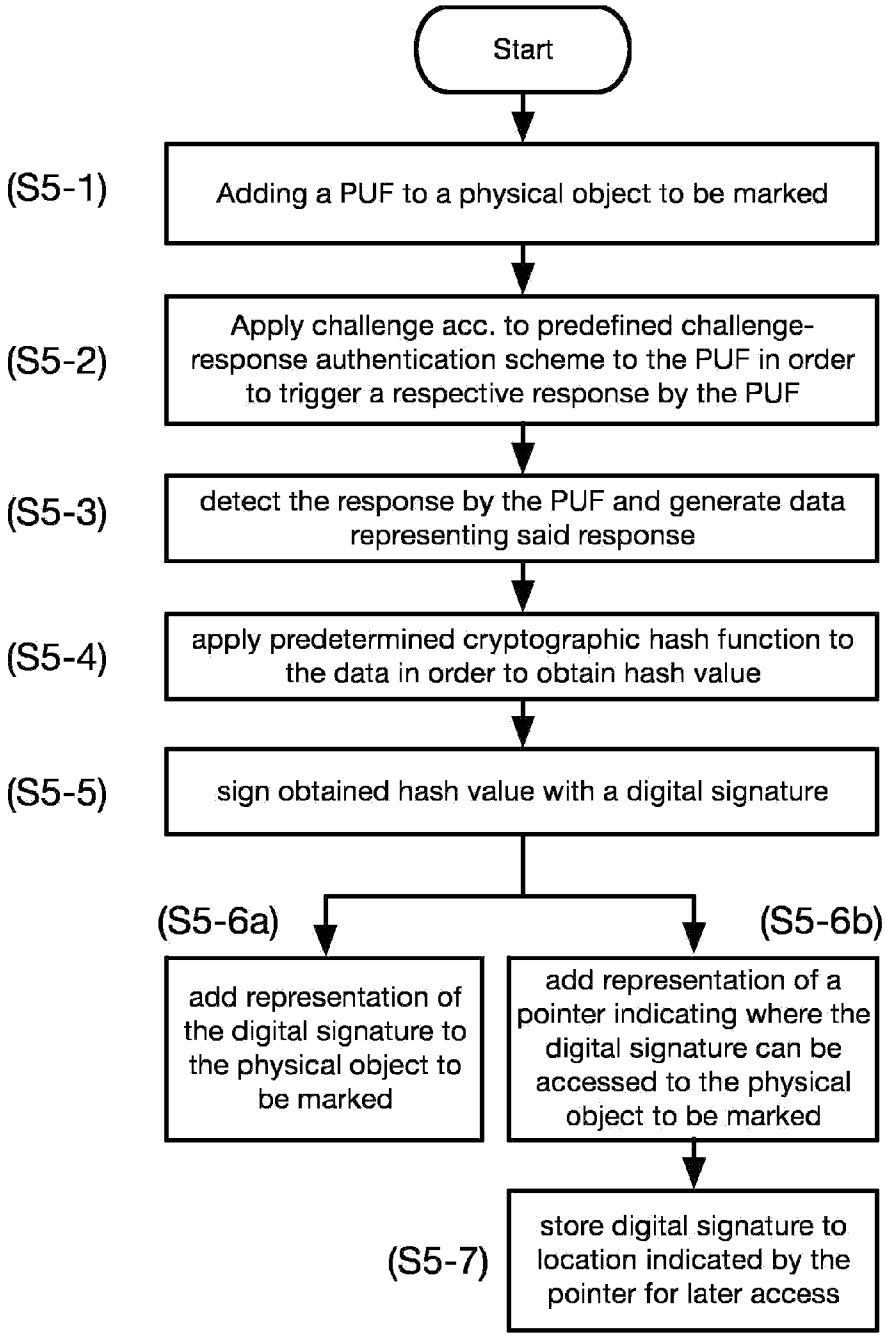
Start
(S5-1)
Adding a PUF to a physical object to be marked
(S5-2)
Apply challenge acc. to predefined challenge-response authentication scheme to the PUF in order to trigger a respective response by the PUF
(S5-3)
detect the response by the PUF and generate data representing said response
(S5-4)
apply predetermined cryptographic hash function to the data in order to obtain hash value
(S5-5)
sign obtained hash value with a digital signature
(S5-6a)
(S5-6b)
add representation of the digital signature to the physical object to be marked
add representation of a pointer indicating where the digital signature can be accessed to the physical object to be marked
(S5-7)
store digital signature to location indicated by the pointer for later access

Fig. 5

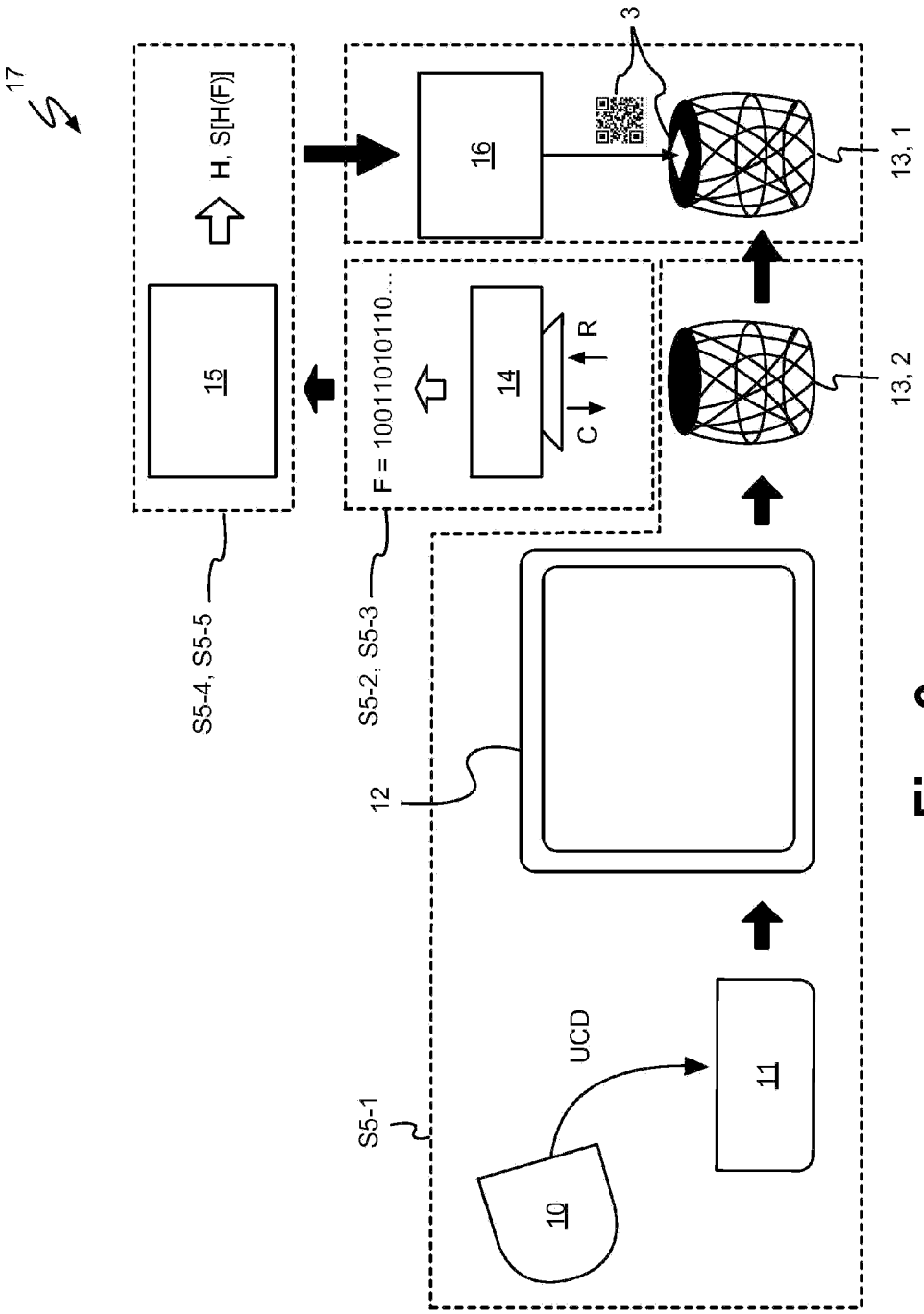
17
H, S[H(F)]
15
16
3
13, 1
F = 10011010110...
14
C
R
13, 2
S5-4, S5-5
S5-2, S5-3
12
S5-1
UCD
11
10

Fig. 6

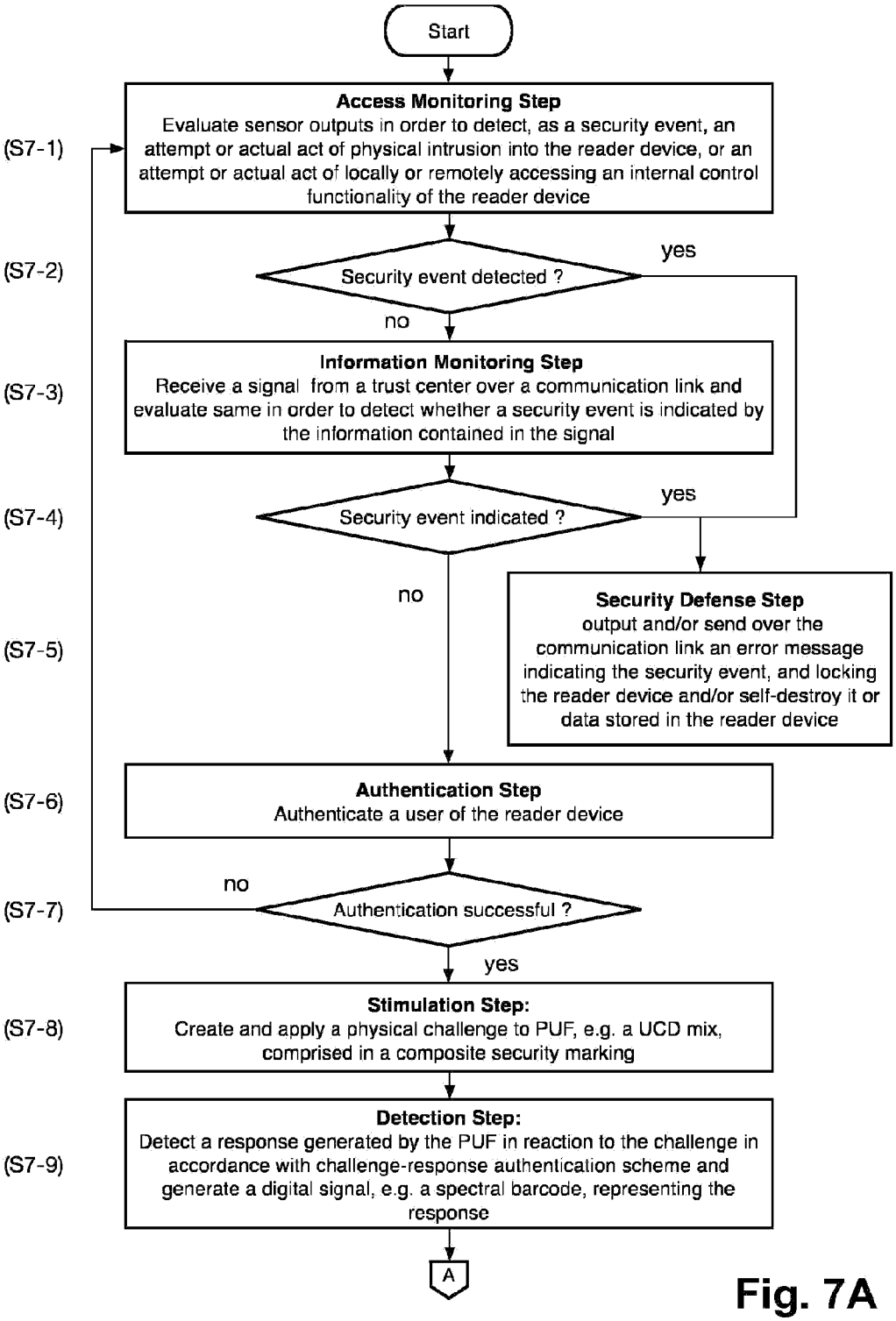
Start
(S7-1)
Access Monitoring Step
Evaluate sensor outputs in order to detect, as a security event, an attempt or actual act of physical intrusion into the reader device, or an attempt or actual act of locally or remotely accessing an internal control functionality of the reader device
(S7-2)
Security event detected ?
yes
no
(S7-3)
Information Monitoring Step
Receive a signal from a trust center over a communication link and evaluate same in order to detect whether a security event is indicated by the information contained in the signal
(S7-4)
Security event indicated ?
yes
no
(S7-5)
Security Defense Step
output and/or send over the communication link an error message indicating the security event, and locking the reader device and/or self-destroy it or data stored in the reader device
(S7-6)
Authentication Step
Authenticate a user of the reader device
(S7-7)
Authentication successful ?
no
yes
(S7-8)
Stimulation Step:
Create and apply a physical challenge to PUF, e.g. a UCD mix, comprised in a composite security marking
(S7-9)
Detection Step:
Detect a response generated by the PUF in reaction to the challenge in accordance with challenge-response authentication scheme and generate a digital signal, e.g. a spectral barcode, representing the response
A

Fig. 7A

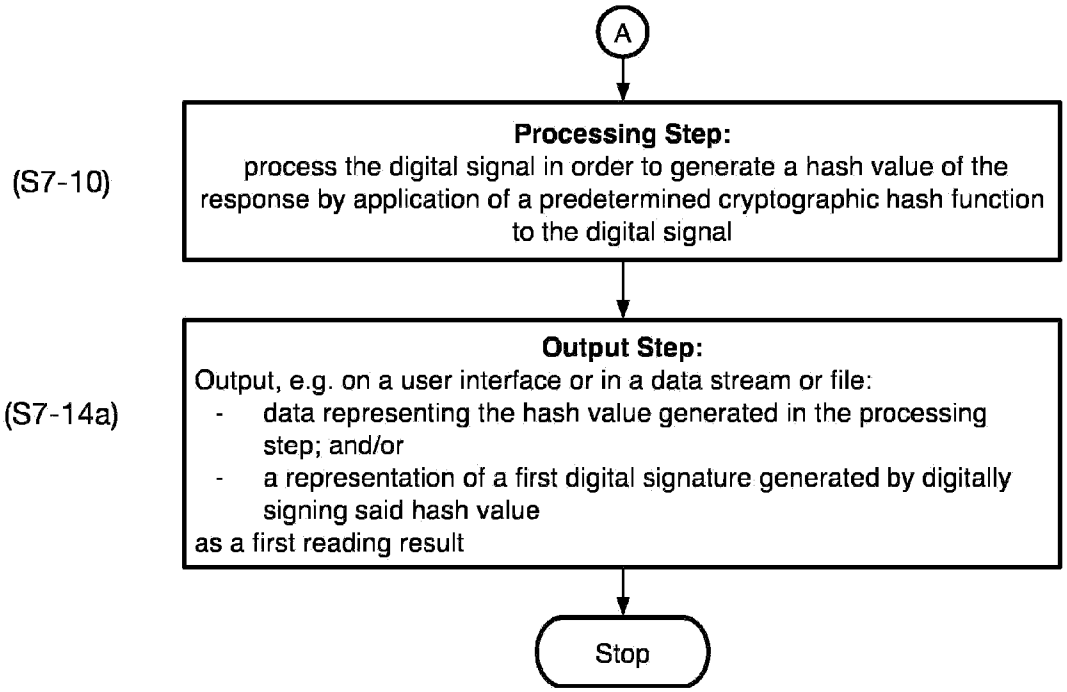
A
(S7-10)
Processing Step:
process the digital signal in order to generate a hash value of the response by application of a predetermined cryptographic hash function to the digital signal
(S7-14a)
Output Step:
Output, e.g. on a user interface or in a data stream or file:
- data representing the hash value generated in the processing step; and/or
- a representation of a first digital signature generated by digitally signing said hash value
as a first reading result
Stop

Fig. 7B

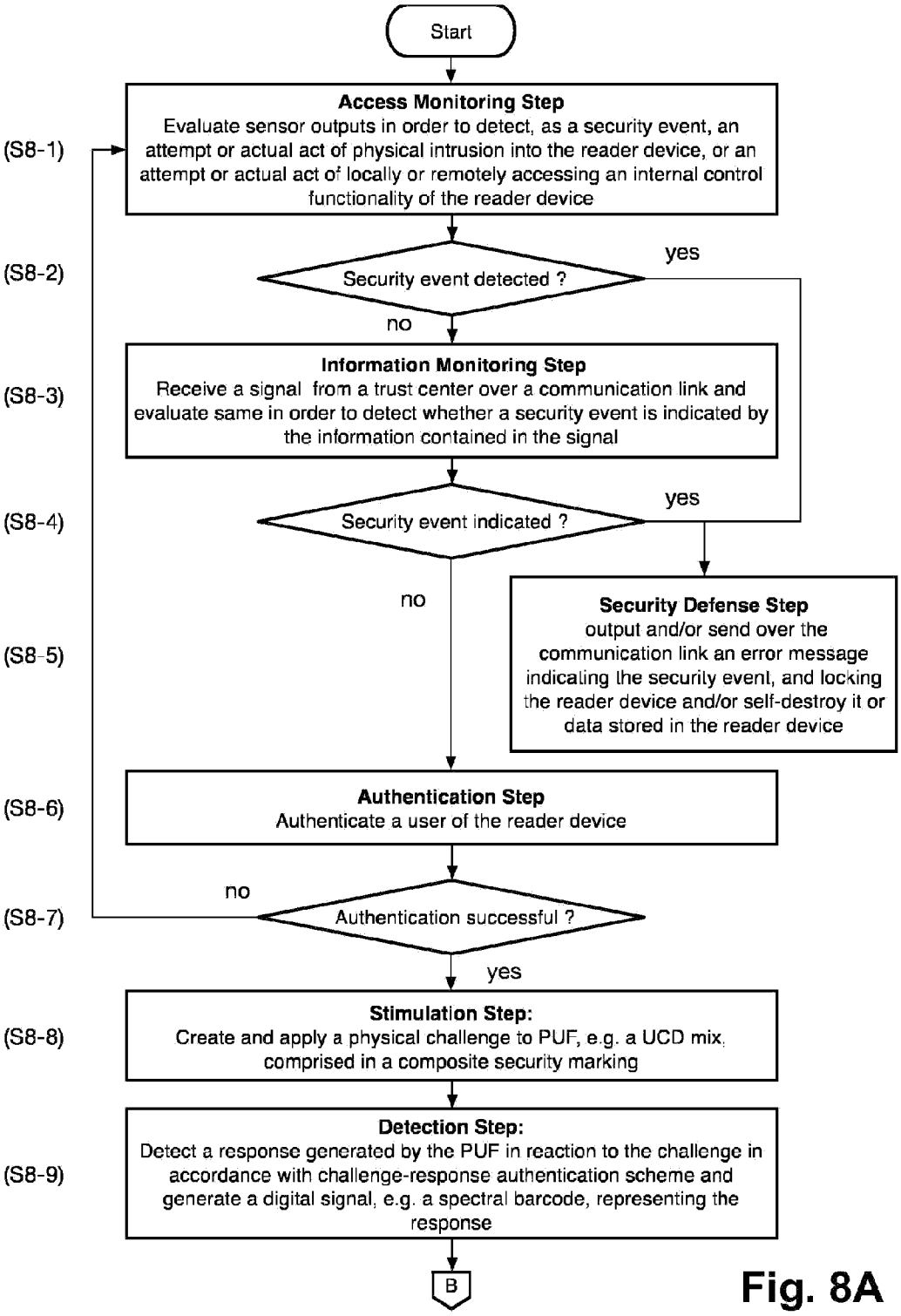
Start
(S8-1)
Access Monitoring Step
Evaluate sensor outputs in order to detect, as a security event, an attempt or actual act of physical intrusion into the reader device, or an attempt or actual act of locally or remotely accessing an internal control functionality of the reader device
(S8-2)
Security event detected ?
yes
no
(S8-3)
Information Monitoring Step
Receive a signal from a trust center over a communication link and evaluate same in order to detect whether a security event is indicated by the information contained in the signal
(S8-4)
Security event indicated ?
yes
no
(S8-5)
Security Defense Step
output and/or send over the communication link an error message indicating the security event, and locking the reader device and/or self-destroy it or data stored in the reader device
(S8-6)
Authentication Step
Authenticate a user of the reader device
(S8-7)
Authentication successful ?
no
yes
(S8-8)
Stimulation Step:
Create and apply a physical challenge to PUF, e.g. a UCD mix, comprised in a composite security marking
(S8-9)
Detection Step:
Detect a response generated by the PUF in reaction to the challenge in accordance with challenge-response authentication scheme and generate a digital signal, e.g. a spectral barcode, representing the response
B

Fig. 8A

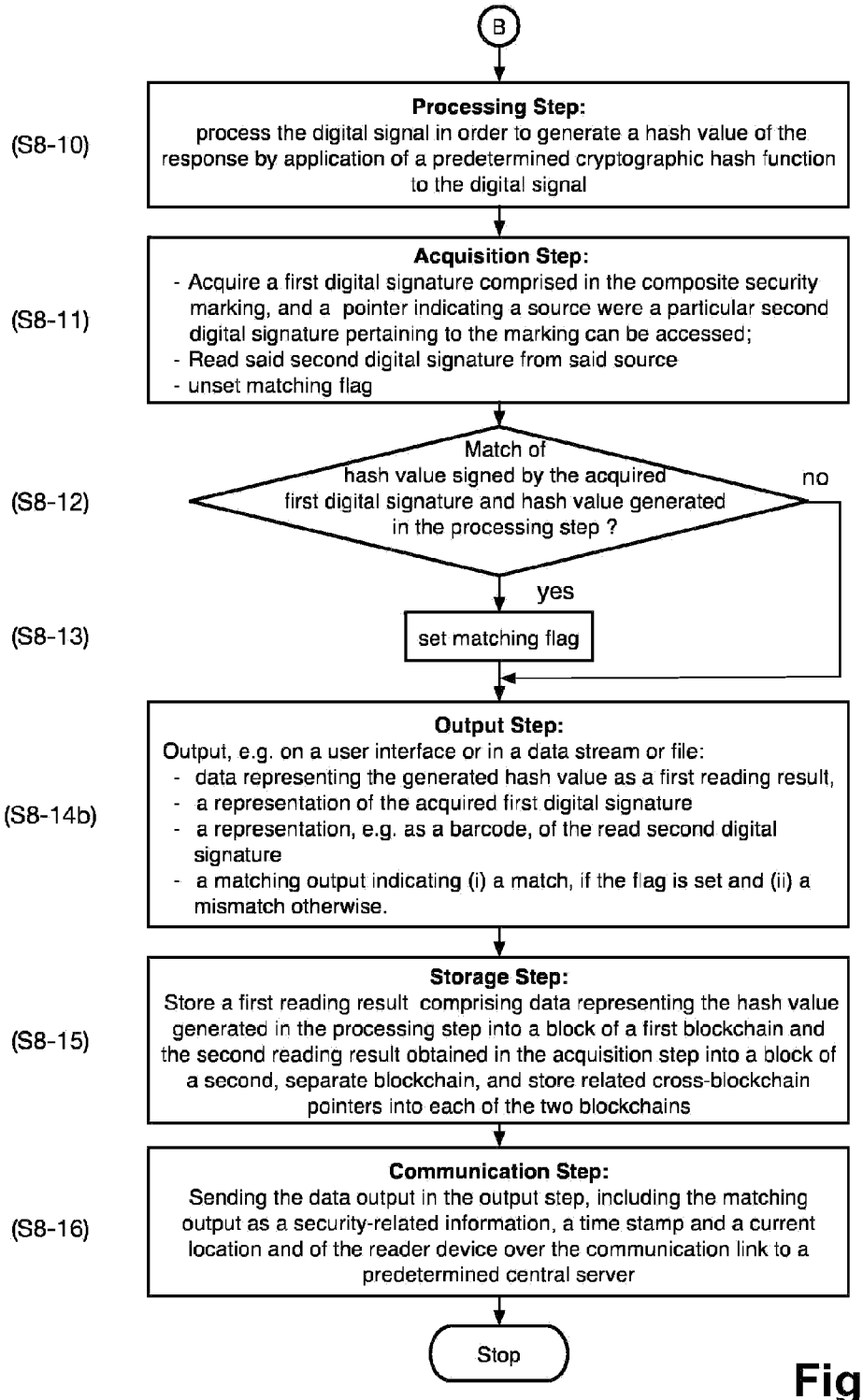
B
(S8-10)
Processing Step:
process the digital signal in order to generate a hash value of the response by application of a predetermined cryptographic hash function to the digital signal
(S8-11)
Acquisition Step:
- Acquire a first digital signature comprised in the composite security marking, and a pointer indicating a source were a particular second digital signature pertaining to the marking can be accessed;
- Read said second digital signature from said source
- unset matching flag
(S8-12)
Match of hash value signed by the acquired first digital signature and hash value generated in the processing step ?
no
yes
(S8-13)
set matching flag
(S8-14b)
Output Step:
Output, e.g. on a user interface or in a data stream or file:
- data representing the generated hash value as a first reading result,
- a representation of the acquired first digital signature
- a representation, e.g. as a barcode, of the read second digital signature
- a matching output indicating (i) a match, if the flag is set and (ii) a mismatch otherwise.
(S8-15)
Storage Step:
Store a first reading result comprising data representing the hash value generated in the processing step into a block of a first blockchain and the second reading result obtained in the acquisition step into a block of a second, separate blockchain, and store related cross-blockchain pointers into each of the two blockchains
(S8-16)
Communication Step:
Sending the data output in the output step, including the matching output as a security-related information, a time stamp and a current location and of the reader device over the communication link to a predetermined central server
Stop

Fig. 8B

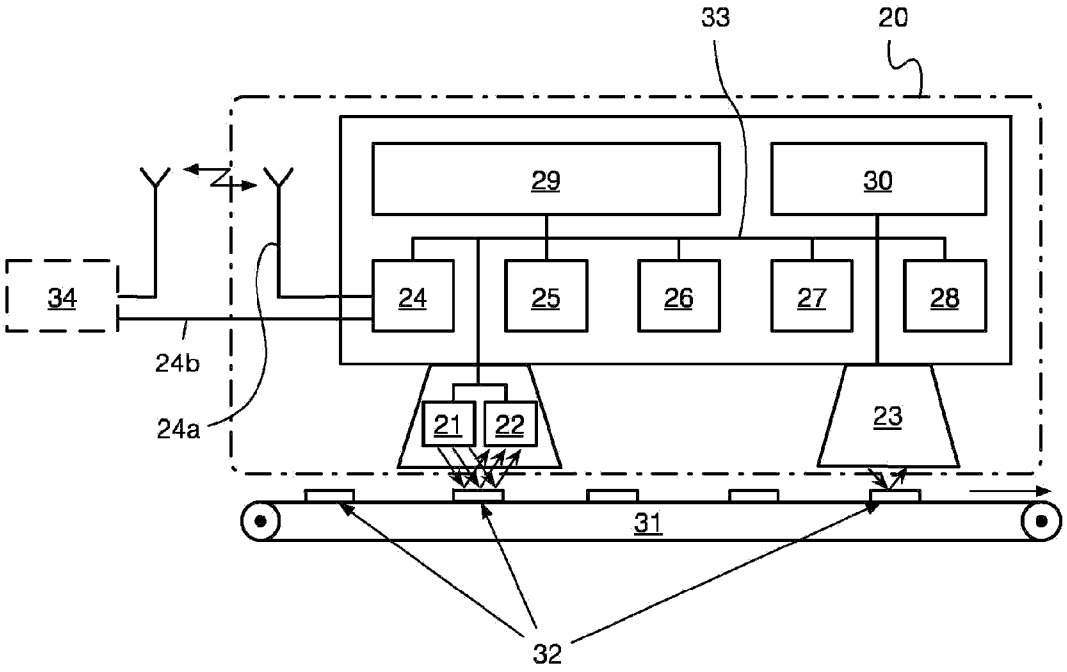

Fig. 9

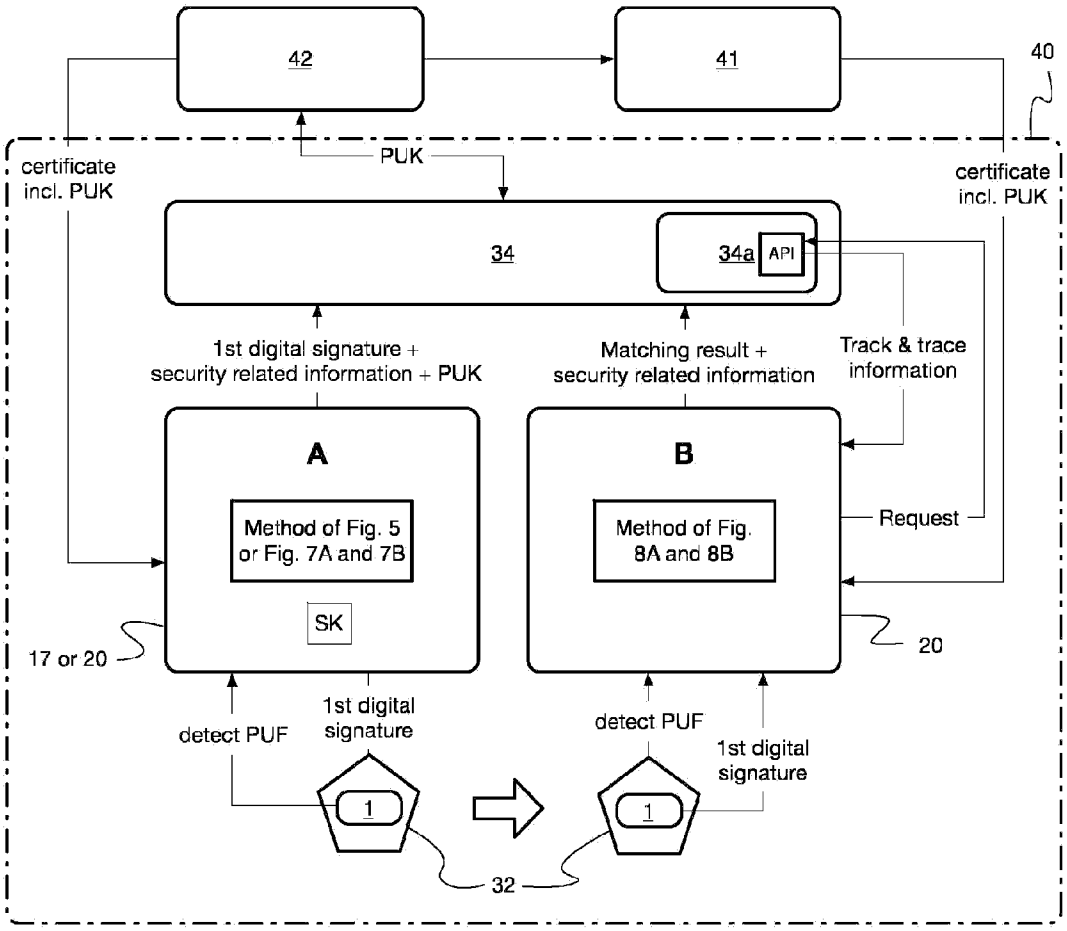
42
41
40
certificate
incl. PUK
PUK
certificate
incl. PUK
34
34a
API
1st digital signature +
security related information + PUK
Matching result +
security related information
Track & trace
information
A
B
Method of Fig. 5
or Fig. 7A and 7B
Method of Fig.
8A and 8B
Request
SK
17 or 20
20
detect PUF
1st digital
signature
detect PUF
1st digital
signature
1
1
32

Fig. 10

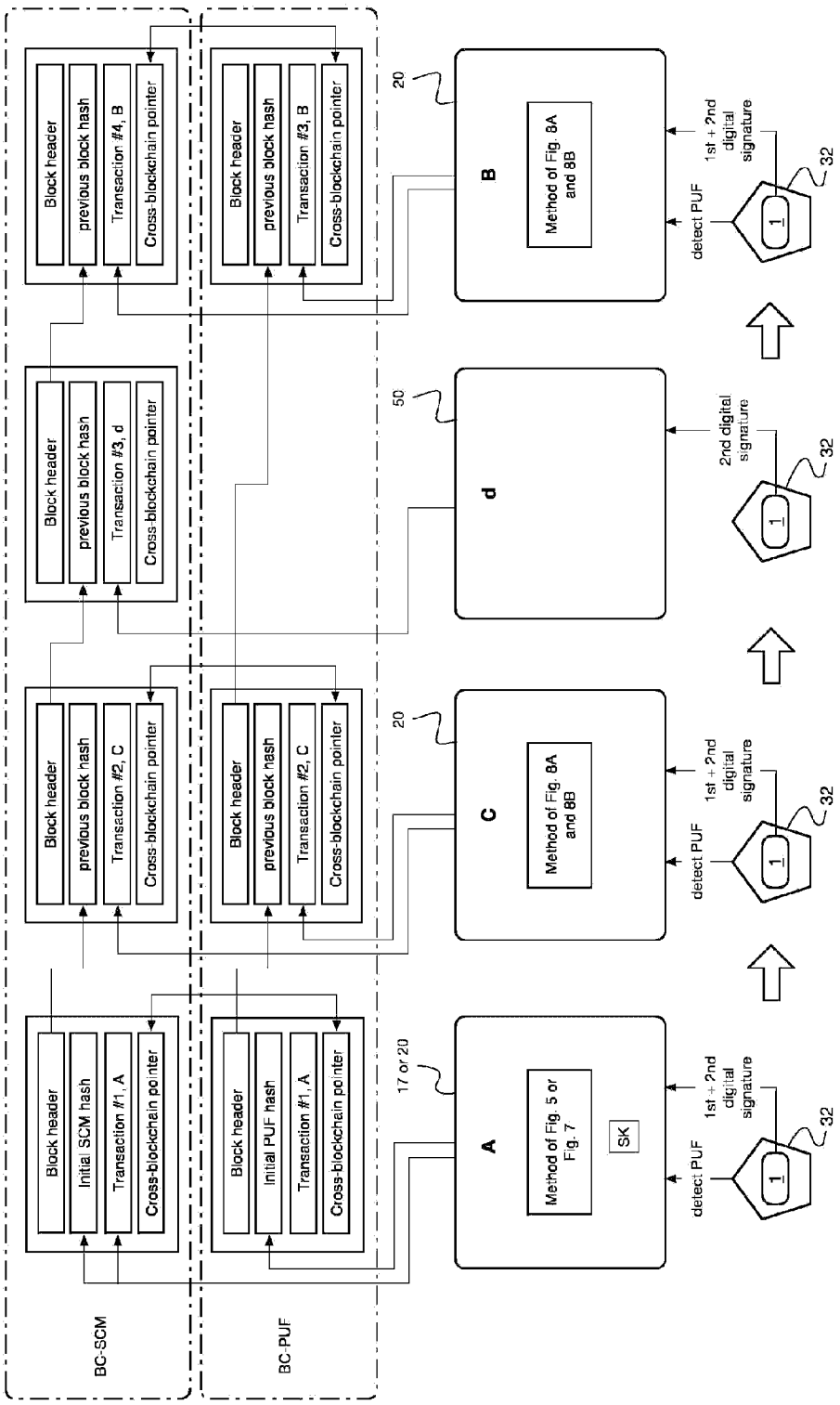
BC-SCM
BC-PUF
Block header
Initial SCM hash
Initial PUF hash
previous block hash
Transaction #1, A
Transaction #2, C
Transaction #3, B
Transaction #3, d
Transaction #4, B
Cross-blockchain pointer
17 or 20
20
50
A
B
C
d
Method of Fig. 5 or Fig. 7
Method of Fig. 8A and 8B
SK
detect PUF
1st + 2nd digital signature
2nd digital signature
32

Fig. 11