Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 3146479 A1 2020/11/12

(21) 3 146 479

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2020/05/08
(87) Date publication PCT/PCT Publication Date: 2020/11/12
(85) Entrée phase nationale/National Entry: 2021/11/05
(86) N° demande PCT/PCT Application No.: FI 2020/050312
(87) N° publication PCT/PCT Publication No.: 2020/225488
(30) Priorité/Priority: 2019/05/09 (FI20197073)

(51) Cl.Int./Int.Cl. *G01D 18/00* (2006.01), *G06F 21/62* (2013.01), *G06F 21/64* (2013.01), *H04L 9/06* (2006.01), *H04L 9/32* (2006.01), *G06F 40/117* (2020.01), *G06F 40/14* (2020.01)

(71) Demandeur/Applicant:
AALTO UNIVERSITY FOUNDATION SR, FI

(72) Inventeurs/Inventors:
AUTIOSALO, JUUSO, FI;
KUOSMANEN, PETRI, FI;
MUSTAPAA, TUUKKA, FI;
NIKANDER, PEKKA, FI

(74) Agent: OYEN WIGGS GREEN & MUTALA LLP

(54) Titre : CERTIFICATION D'UN RESULTAT DE MESURE D'UN DISPOSITIF DE MESURE
(54) Title: CERTIFICATION OF A MEASUREMENT RESULT OF A MEASURING DEVICE

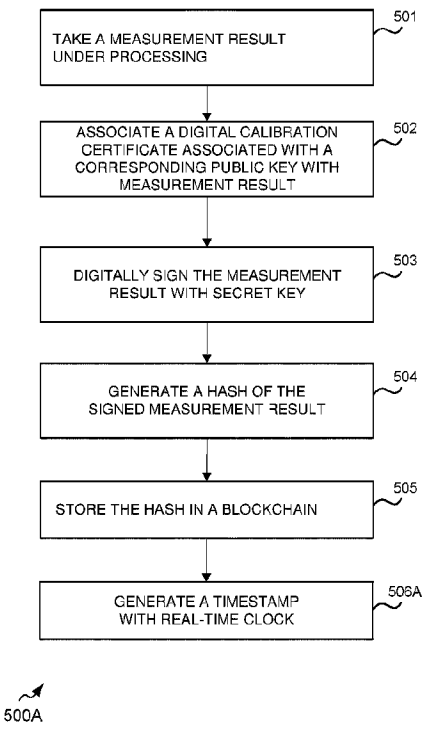

FIG. 3A

(57) Abrégé/Abstract:
The invention enables the certification of a measurement result of a measuring device. A measuring device arranged in connection with a data security module according to the invention takes under processing a measurement result produced using a measuring instrument of the measuring device (501). The measuring device associates a digital calibration certificate associated with a public key corresponding to a secret key stored in a key storage with the measurement result taken under processing (502). The measuring device digitally signs the associated measurement result using a signing function of the data security module and the secret key stored in the key storage (503).

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 November 2020 (12.11.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/225488 A1

(51) International Patent Classification:
G01D 18/00 (2006.01) *H04L 9/32* (2006.01)
G06F 21/62 (2013.01) *G06F 40/117* (2020.01)
G06F 21/64 (2013.01) *G06F 40/14* (2020.01)
H04L 9/06 (2006.01)

(21) International Application Number:
PCT/FI2020/050312

(22) International Filing Date:
08 May 2020 (08.05.2020)

(25) Filing Language: Finnish

(26) Publication Language: English

(30) Priority Data:
20197073 09 May 2019 (09.05.2019) FI

(71) Applicant: **AALTO UNIVERSITY FOUNDATION SR** [FI/FI]; P.O. Box 11000, 00076 Aalto (FI).

(72) Inventors: **AUTIOSALO, Juuso**; c/o AALTO UNIVERSITY FOUNDATION SR, P.O. Box 11000, 00076 Aalto (FI). **KUOSMANEN, Petri**; c/o AALTO UNIVERSITY FOUNDATION SR, P.O. Box 11000, 00076 Aalto (FI). **MUSTAPÄÄ, Tuukka**; c/o AALTO UNIVERSITY FOUNDATION SR, P.O. Box 11000, 00076 Aalto (FI). **NIKANDER, Pekka**; c/o AALTO UNIVERSITY FOUNDATION SR, P.O. Box 11000, 00076 Aalto (FI).

(74) Agent: **PAPULA OY**; P.O. Box 981, 00101 Helsinki (FI).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: CERTIFICATION OF A MEASUREMENT RESULT OF A MEASURING DEVICE

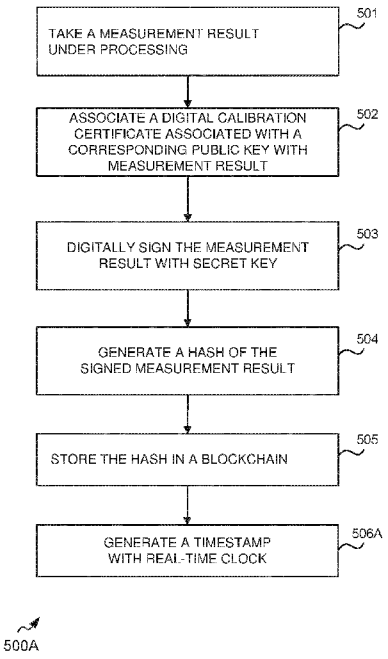

FIG. 3A

(57) Abstract: The invention enables the certification of a measurement result of a measuring device. A measuring device arranged in connection with a data security module according to the invention takes under processing a measurement result produced using a measuring instrument of the measuring device (501). The measuring device associates a digital calibration certificate associated with a public key corresponding to a secret key stored in a key storage with the measurement result taken under processing (502). The measuring device digitally signs the associated measurement result using a signing function of the data security module and the secret key stored in the key storage (503).

WO 2020/225488 A1

[Continued on next page]

WO 2020/225488 A1

Published:
— *with international search report (Art. 21(3))*

CERTIFICATION OF A MEASUREMENT RESULT OF A MEASURING DEVICE

FIELD OF THE INVENTION

The invention relates to measuring devices and specifically to the certification of a measurement result of a measuring device.

STATE OF THE ART

With accelerating digitalization and automatization the need for new solutions to improve reliable and wide access to digital measurement data is great. At present the calibration certificates of measuring devices are either paper documents or PDF (portable document format) documents which are electronic, but in content equivalent to the paper documents, and which are not machine-understandable. Essentially the only benefit they provide to the user of the measuring device is documenting the verification of the accuracy of the measuring device relative to a national measurement standard. The added value provided by the existing analogue certificates has up to the present been almost exclusively that of quality control.

Currently there is no digital calibration certificate in which strong and secure authentication would be combined in a way proving that the calibration information belongs with certainty to a specific measuring device.

SUMMARY OF THE INVENTION

According to a first aspect of the present invention, a data security module is disclosed. The data security module comprises a key storage which is configured to store a cryptographic key in a protected manner, such that said cryptographic key is usable in-

ternally in the data security module without being accessible from outside of the data security module. The data security module further comprises a signing function which is configured to perform digital signing using the cryptographic key stored in the key storage. The data security module further comprises a certificate storage which is configured to store at least a part of a digital calibration certificate associated with a measuring device associated with the data security module, such that the at least part of the digital calibration certificate is accessible from outside of the data security module. The cryptographic key stored in the key storage is a secret key of a public key cryptography key pair associated with the measuring device, and the at least part of the digital calibration certificate stored in the certificate storage is associated with a public key corresponding to the secret key.

In an embodiment of the invention, the data security module further comprises a physically unclonable function (PUF) for generating the secret key during runtime.

In an embodiment of the invention, the data security module further comprises a real-time clock.

In an embodiment of the invention, the data security module further comprises a communication function for external communication of the data security module.

In an embodiment of the invention, the protection of the key storage is implemented on a hardware level.

In an embodiment of the invention, the signing function is implemented at least partly on a hardware level.

In an embodiment of the invention, the at least part of the digital calibration certificate stored in the certificate storage comprises the public key.

In an embodiment of the invention, the at least part of the digital calibration certificate stored in the certificate storage comprises identity information associated with the public key.

According to a second aspect of the present invention, a measuring device arranged in connection with the data security module according to the first aspect of the invention is disclosed. The measuring device comprises a measuring instrument, at least one processor, and at least one memory which comprises computer program code. The at least one memory and the computer program code are configured with the at least one processor to cause the measuring device to:

take under processing a measurement result produced using the measuring instrument;

associate a digital calibration certificate associated with a public key corresponding to a secret key stored in a key storage of the data security module with the measurement result taken under processing; and

digitally sign the associated measurement result using a signing function of the data security module and the secret key stored in the key storage.

In an embodiment of the invention, the at least one memory and the computer program code are further configured with the at least one processor to cause the measuring device to perform the association of the digital calibration certificate with the measurement result taken under processing by generating a hash of the digital calibration certificate and by including the generated hash in the measurement result taken under processing.

In an embodiment of the invention, the at least one memory and the computer program code are further configured with the at least one processor to cause the measuring device to generate a hash of the signed measurement result and store the generated hash in a blockchain.

In an embodiment of the invention, the data security module comprises a real-time clock and the at least one memory and the computer program code are further configured with the at least one processor to cause the measuring device to generate a timestamp for the signed measurement result using the real-time clock.

In an embodiment of the invention, the at least one memory and the computer program code are further configured with the at least one processor to cause the measuring device to generate a timestamp for the signed measurement result using eIDAS (Electronic Identification, Authentication and Trust Services).

In an embodiment of the invention, the at least one memory and the computer program code are further configured with the at least one processor to cause the measuring device to protect communication with an external third party.

According to a third aspect of the present invention, a method of certification of a measurement result of a measuring device is disclosed. The method comprises the steps of:

taking under processing, by the measuring device, a measurement result produced using the measuring device;

associating, by the measuring device, a digital calibration certificate with the measurement result taken under processing, the digital calibration certificate associated with a public key corresponding to a secret key stored in a key storage of the data security module according to the first aspect of the invention configured in connection with the measuring device; and

digitally signing, by the measuring device, the associated measurement result using a signing function of the data security module and the secret key stored in the key storage.

In an embodiment of the invention, the association of the digital calibration certificate with the

measurement result taken under processing is performed by generating a hash of the digital calibration certificate and by including the generated hash in the measurement result taken under processing.

In an embodiment of the invention, the method further comprises generating, by the measuring device, a hash of the signed measurement result and storing, by the measuring device, the generated hash in a blockchain.

In an embodiment of the invention, the data security module comprises a real-time clock and the method further comprises generating, by the measuring device, a timestamp for the signed measurement result using the real-time clock.

In an embodiment of the invention, the method further comprises generating, by the measuring device, a timestamp for the signed measurement result using eIDAS (Electronic Identification, Authentication and Trust Services).

According to a fourth aspect of the present invention, a computer program product is disclosed, which computer program product comprises at least one computer-readable storage medium which comprises a set of instructions which, when executed by one or more processors, cause a measuring device to perform the method according to the third aspect of the invention.

With the solution according to the invention the manufacturers of devices producing measurement results may easily and cost-efficiently attach to their products a functionality by means of which the devices automatically sign the produced measurement results using a digital calibration certificate defined for the device during or after manufacture as a certificate of signing of the measurement results. At least some of the solutions according to the invention enable the signing of measurement results to be performed in a way enabling

the measurement results to be offered for purchasing by other organizations in a data market.

Replacing conventional calibration certificates with digital calibration certificates provides the advantage of improving the quality and reusability of measurement data, as digital certificates enable the accuracy, measurement conditions and authenticity of the data to be certified. Because it has so far been problematic to certify the Internet of Things (IoT) based IOT data, and because there is no clear solution for it, the use of digital calibration certificates as the certificates also significantly improves the quality of data of IoT systems processing measurement data and the reliability of the results obtained.

At least some of the solutions according to the invention are useful e.g. for measuring device and IoT device manufacturers, because they enable the device manufacturers to quickly and easily implement new standards and because they enable the implementation of necessary technology already before completion of the standard, such that devices existing in the market already may easily be updated according to the standard. Further, at least some of the solutions according to the invention are useful for device owners, because by means of the solutions the device owners may quickly and easily introduce the data produced by the device into a data market.

LIST OF FIGURES

Below the invention will be described by means of the following examples of its embodiments with reference to the accompanying drawing, in which

Fig. 1 is a schematic illustration of a system according to the invention;

Fig. 2A is a block diagram of a data security module according to the invention;

Fig. 2B is a block diagram of a measuring device according to the invention;

Fig. 2C is a block diagram of another measuring device according to the invention;

Fig. 3A is a flow diagram of a method according to the invention; and

Fig. 3B is a flow diagram of another method according to the invention.

The same reference numbers are used throughout the accompanying drawing to refer to the corresponding elements.

DETAILED DESCRIPTION OF THE INVENTION

Below is a detailed description of embodiments of the present invention, examples of which are illustrated in the accompanying drawings. The following detailed description together with the accompanying drawing are intended to illustrate the examples, and are not intended to represent the only forms in which the presented examples may be implemented or utilized. In the following, example functions and sequences of steps/operations for combining and using the examples will be disclosed. However, the same or equivalent functions and steps/operations may also be accomplished with other examples.

The advantage of digital calibration certificates is their machine-processability. This enables the utilization of the information contained by the certificates in other automatized systems. In addition, by means of digital calibration certificates the measurement data produced by measuring devices can be better protected by using the calibration certificate as a certificate of the digital signatures used for protecting the measurement data, which helps to solve problems in the verification of authenticity, integrity, measurement accuracy and other reliability of the data.

The signing of accuracy, integrity, reliability and authenticity of data enables a broad data market to be formed, as the users of measuring devices may sell the signed data for use by other organizations. Such situations may encompass e.g. the selling of anonymized car outdoor temperature data and position information for the providers of weather services. According to studies, by the mere reuse of data and analytics within one company, an improvement of 3-7% in productivity may be achieved. When data may be reliably combined from many different sources and over company boundaries, at a general estimate on average a corresponding and in the best case a multiple improvement in productivity may be achieved.

Fig. 1 illustrates, by way of example, components of a system 1000 according to the invention, in which system 1000 various embodiments of the present invention may be implemented. In the example of Fig. 1 there is illustrated a measuring device 200, in connection with which a data security module 100 according to the invention is arranged. In the example of Fig. 1 the measuring device 200 is in communication connection (by wireless and/or wired means) with a communications network 300 (such as the Internet), and thereby with one or more third party apparatuses 400 which are also connected to the communications network 300. Examples of the third party 400 include an eIDAS (Electronic Identification, Authentication and Trust Services) provider, a real-time clock synchronization server, providers of measurement data related services, providers of data markets, other users of measuring devices etc. The arrangement illustrated in Fig. 1 enables the certification of a measurement result of the measuring device 200 and forwarding of the certified measurement result further for various applications, as will be explained in more detail below. The measuring device 200

illustrated in Fig. 1 corresponds to the measuring device 200A illustrated in Fig. 2B and to the measuring device 200B illustrated in Fig. 2C.

Fig. 2A is a block diagram of a data security module 100 according to the invention.

The data security module 100 described below may, for example, be implemented as a data security module which includes hardware and/or software and which may be provided as part of the measuring device 200A producing measurement results or connected between the measuring device 200B producing measurement results and the communications network 300. The data security module 100 may also be implemented as a software module provided as part of the software of the measuring device 200A producing measurement results such that it utilizes a hardware-level data security module existing in the measuring device 200A (not illustrated in Fig. 2B), for example a so-called trusted execution environment which is integrated in a processor 202 of the measuring device 200A and which may be for example SGX from Intel or TrustZone from ARM. The data security module 100 may also be implemented as a software component without a hardware-level data security module, if the measuring device 200A in which the data security module 100 is incorporated is as a whole considered sufficiently secure, for example because the hardware is fully sealed. This may be the situation for example if the measuring device 200A is itself able to detect the breakage of the seal and store information on the breakage of the seal such that the information may not be deleted.

An embodiment of the data security module 100 may be a dedicated, integrated and/or packaged microcircuit which may be designed such that it is easily integratable as part of the measuring device 200A producing measurement results. The microcircuit according to this embodiment may include one or more of the sub-

components described below, implemented by way of hardware. The microcircuit may be implemented by technology preventing the cryptographic keys and/or other information stored thereon from being read and/or exposed (so-called tamper proof technology).

In an embodiment, the various components of the data security module 100, such as a key storage 110, a signing function 120, a certificate storage 130, a PUF 140, a real-time clock 150 and/or a communication function 160 are configured to communicate with each other via or by means of a communication connection 170, such as a bus. In an embodiment, between the signing function 120 and the key storage 110 there is arranged a direct communication connection 180 separate from the communication connection 170. In an embodiment, between the PUF 140 and the key storage 110 there is arranged a direct communication connection 190 separate from the communication connection 170.

In an embodiment, the data security module 100 may also comprise a processor and/or a memory (not illustrated in Fig. 2A). This arrangement may be advantageous for example in the example of Fig. 2C in which the data security module 100 is implemented as an external module with respect to the measuring device 200B.

The data security module 100 comprises a key storage 110 which is configured to store a cryptographic key in a protected manner, i.e. such that said cryptographic key is usable internally in the data security module 100 without being accessible from outside of the data security module 100 (in other words, such that said cryptographic key cannot be for example read, copied or forwarded from/to outside of the data security module 100). In an embodiment of the invention, this protection of the key storage 110 is implemented on a hardware level.

The data security module 100 further comprises a signing function 120 which is configured to perform

digital signing using the cryptographic key stored in the key storage 110. In an embodiment of the invention, the signing function 120 is implemented at least partly on a hardware level. In an embodiment, the direct communication connection 180 separate from the bus 170, arranged between the signing function 120 and the key storage 110, enables the signing function 120 to use a secret key 111 (for example read the contents of the secret key 111). In this embodiment, the secret key 111 cannot be read via the communication connection 170.

The data security module 100 further comprises a certificate storage 130 which is configured to store at least a part of a digital calibration certificate (DCC) 131 associated with the measuring device 200A, 200B (described in more detail below in connection with Fig. 2B-2C) associated with the data security module 100 such that this at least part of the digital calibration certificate 131 is accessible from outside of the data security module 100 (in other words, such that this at least part of the digital calibration certificate 131 can be for example read, copied and/or forwarded from/to outside of the data security module 100).

In an example the certificate storage 130 may require that when the certificate 131 is being updated, the new certificate version must be a newer version of the certificate which is already stored in the storage 130. This may be implemented for example such that the storage 130 requires that the new certificate includes a cryptographic or other hash of the old certificate, and that the new certificate is signed with at least a same key as the certificate stored in the storage 130.

The cryptographic key stored in the key storage 110 is the secret key 111 of a public key cryptography key pair of associated with the measuring device 200A, 200B, and the at least part of the digital calibration certificate 131 stored in the certificate storage 130 is associated with a public key 132 corresponding to the

secret key 111. In an embodiment of the invention, the feature that the at least part of the digital calibration certificate 131 stored in the certificate storage 130 is associated with the public key 132 corresponding to the secret key 111 comprises that the at least part of the digital calibration certificate 131 stored in the certificate storage 130 comprises this public key 132. In another embodiment of the invention, the feature that the at least part of the digital calibration certificate 131 stored in the certificate storage 130 is associated with the public key 132 corresponding to the secret key 111 comprises that the at least part of the digital calibration certificate 131 stored in the certificate storage 130 comprises identity information associated with this public key 132. The public key 132 may be accessed by means of the identity information associated with the public key 132.

In an embodiment of the invention, the data security module 100 further comprises a PUF (physical unclonable function or physically unclonable function) 140 for generating the secret key 111 during runtime. Thereby the secret key 111 may be produced in a secure manner (for example when the data security module 100 and/or the measuring device 200A starts up) without having to permanently store the secret key 111 in the data security module 100. In an embodiment, the direct communication connection 190 separate from the bus 170, which is arranged between the PUF 140 and the key storage 110, enables the PUF 140 to write the secret key 111 in the key storage 110. In this embodiment, the secret key 111 cannot be written via the communication connection 170. In another embodiment there is no communication connection 190, but data security is arranged such that the PUF 140 does not disclose the generated secret key 111 except once (for example when the secret key 111 is written in the key storage 110 after start-up).

In an embodiment of the invention, the data security module 100 further comprises a real-time clock 150. The real-time clock 150 may, for example, be used for attaching a timestamp to the measurement results, which timestamp may be part of the information which is certified by signing.

In an embodiment of the invention, the data security module 100 further comprises a communication function 160 for external communication of the data security module. By means of the communication function 160 the data security module 100 may for example communicate with the outside world and for example verify that the real-time clock 150 of the data security module 100 runs in universal time. The communication function 160 may be protected from other software and hardware of the data security module 100 and/or the measuring device 200A such that the data security module 100 may verify that the communication is with an external service, for example an Internet-based service, the identity and for example a cryptographic identifier of which may be stored in the data security module 100, for example in the certificate storage 130 when this cryptographic identifier is a public key or in the key storage 110 when this cryptographic identifier is a secret key.

In this text the term “storage” refers to a memory which is used for a specific purpose and to which functions have been linked. In an example, the key storage 110 is thereby a memory which is located in the data security module 100 and to which it is possible to write (for changing a key) but which cannot be read. The reading of the memory 110 has been prevented at a hardware level, for example such that there are no circuits needed for reading in the hardware. The signing function (for example a separate logic circuit) 120 is linked to the memory 110, to which signing function a processor using the data security module 100 (such as the processor 202 in the example of Fig. 2B or the external data

security module's 100 own processor in the example of Fig. 2C) may input, i.e. write, a document to be signed (i.e. for example a combination of a measurement result and the digital calibration certificate 131 or a hash of the calibration certificate 131) and from which signing function it may after some time read the digital signature corresponding to the document in question.

Fig. 2B is a block diagram of a measuring device 200A according to the invention.

The measuring device 200A is arranged in connection with the data security module 100. In the example of Fig. 2B this means that the data security module 100 is integrated as a part of the measuring device 200A. The data security module 100 may, for example, be a microcircuit or another hardware-based implementation. Alternatively, the data security module 100 may be implemented as a part of the software of the measuring device 200A. Alternatively, the data security module 100 may be implemented as partly hardware and partly software. In an example, the measuring device 200A comprises an IoT (Internet of Things) measuring device.

The measuring device 200A comprises a measuring instrument 201 (such as a sensor or the like), at least one processor 202, and at least one memory 204 which comprises computer program code 205.

Although the measuring device 200A of Fig. 2B is illustrated as comprising only one processor 202, the measuring device 200A may comprise a plurality of processors. In an embodiment, the computer program code 205 may comprise instructions 205 (e.g. an operating system and/or various applications). In addition, stored instructions may be executed by the processor 202. In an embodiment, the processor 202 may be embodied as a multi-core processor, a single-core processor, or a combination of one or more multi-core processors and one or more single-core processors. The processor 202 may,

for example, be embodied as one or more of various processing devices, such as a coprocessor, a microprocessor, a controller, a DSP (digital signal processor), a processing circuitry with or without a DSP, or various other processing devices including an ASIC (application specific integrated circuit), an FPGA circuit (field programmable gate array), a microcontroller unit, a hardware accelerator, or the like. In an embodiment, the processor 202 may be configured to execute a hardcoded functionality. In an embodiment, the processor 202 is embodied as an executor of software instructions, wherein the processor 202 may be configured with the instructions to execute the algorithms and/or operations described in this disclosure when the instructions are executed.

The memory 204 may be embodied as one or more volatile memory devices, one or more non-volatile memory devices, and/or a combination of one or more volatile memory devices and one or more non-volatile memory devices. The memory 204 may, for example, be embodied as a semiconductor memory such as, for example, a PROM (programmable ROM), an EPROM (erasable PROM), a flash ROM, a RAM (random access memory) etc.

In an embodiment, various components of the measuring device 200A, such as the measuring instrument 201, the processor 202, the memory 204, and/or the data security module 100 are configured to communicate with each other via or by means of a communication connection 203, such as a bus. The communication connection 203 may be arranged for example on a printed circuit board, such as a mother board or the like.

The measuring device 200A illustrated and described herein is only an example of a device which may utilize the embodiments of the invention, and it is not intended to limit the scope of protection of the invention. It is to note that the measuring device 200A may

comprise more or fewer components than what is illustrated in Fig. 2. The measuring device 200A may be distributed into several different physical entities communicating with each other by means of a suitable communication connection.

The at least one memory 204 and the computer program code 205 are configured with the at least one processor 202 to cause the measuring device 200A to take under processing a measurement result produced using the measuring instrument 201.

The at least one memory 204 and the computer program code 205 are further configured with the at least one processor 202 to cause the measuring device 200A to associate the digital calibration certificate 131 associated with the public key 132 corresponding to the secret key 111 stored in the key storage 110 of the data security module 100 with the measurement result taken under processing. In an example embodiment of the invention, the at least one memory 204 and the computer program code 205 are configured with the at least one processor 202 to cause the measuring device 200A to perform this association of the digital calibration certificate 131 with the measurement result taken under processing by generating a hash of the digital calibration certificate 131 and by including the generated hash in the measurement result taken under processing. In an example embodiment, in addition to and/or instead of a hash of the digital calibration certificate 131, a suitable identifier of the calibration certificate 131 may be included in the measurement result taken under processing.

A simplified example of presenting the measurement result in an XML (extensible markup language) code is:

```
<measurement-result>...</measurement-result>
```

Then the same XML code for the measurement result is for example as follows when the calibration certificate is associated with it:

```
<measurement-result-with-associated-calibration-certificate>
<measurement-result>...</measurement-result>
<associated-calibration-certificate>
<calibration-certificate-identifier>...</calibration-certificate-identifier>
<calibration-certificate-fingerprint>...</calibration-certificate-fingerprint>
</associated-calibration-certificate>
</measurement-result-with-associated-calibration-certificate>
```

In this example an identifier and a digital hash of the calibration certificate are attached to / included in the measurement result.

The at least one memory 204 and the computer program code 205 are further configured with the at least one processor 202 to cause the measuring device 200A to digitally sign the associated measurement result using the signing function of the data security module 100and the secret key 111 stored in the key storage 110.

Continuing the example presented above, the XML code for the measurement result is for example as follows after signing:

```
<signed-measurement-result>
<measurement-result-with-associated-calibration-certificate>
<measurement-result>...</measurement-result>
<associated-calibration-certificate>
<calibration-certificate-identifier>...</calibration-certificate-identifier>
```

<calibration-certificate-fingerprint>...</calibration-certificate-fingerprint>
</associated-calibration-certificate>
</measurement-result-with-associated-calibration-certificate>
<digital-signature>...</digital-signature>
</signed-measurement-result>

In an embodiment of the invention, the at least one memory 204 and the computer program code 205 are further configured with the at least one processor 202 to cause the measuring device 200A to generate a hash of the signed measurement result and store the generated hash in a blockchain. The blockchain used may be for example ethereum or hyperledger fabric. Storing the generated hash of the signed measurement result in a blockchain provides for example the advantage of indicating that the measurement result was at the latest created when storing in the blockchain was performed, because the blockchain cannot be changed afterwards. In other words, by using a blockchain a so-called notarized timestamp may be provided.

In an embodiment of the invention, the data security module 100 comprises a real-time clock 150 and the at least one memory 204 and the computer program code 205 are further configured with the at least one processor 202 to cause the measuring device 200A to generate a timestamp for the signed measurement result using the real-time clock 150. The timestamp produced using the real-time clock 150 may be used, for example, as an alternative for a timestamp produced using a blockchain.

In an embodiment of the invention, the at least one memory 204 and the computer program code 205 are further configured with the at least one processor 202 to cause the measuring device 200A to generate a timestamp for the signed measurement result using eIDAS

(Electronic Identification, Authentication and Trust Services). eIDAS is a regulation of the European Union (EU) on electronic trust services including e.g. an electronic timestamp which is a timestamp attached to an electronic signature and which certifies the time of signing, or at least the time before which the signing was performed, if timestamping is made afterwards.

By means of the data security module 100 the measuring device 200A, 200B containing or otherwise being linked to the module may be strongly identified, using for example the secret key 111 corresponding to the public key 132 stored in the certificate storage 130 or the secret key produced using the PUF 140 for the signing of suitable identification information. The identification information may be for example produced by the measuring device 200A or the data security module 100 or it may form part of an identification protocol in which the identification information or part of it is obtained from outside of the measuring device 200A by means of a communication connection.

By means of the data security module 100 the measurement results produced by the measuring device 200A, 200B may for example be signed in such a way that the user of the measurement results may, for example: a) check which measuring device has produced the results, b) at which time (date and time) the results have been produced and/or signed, c) that the results have not been changed after the measuring device 200A has signed them, d) what calibration certificate 131 has been stored in the measuring device 200A, 200B when the results were signed, e) what was or were the current measurement uncertainty or uncertainties on the basis of the calibration certificate 131 when the measurement was performed and/or signed. This type of signing together with the calibration certificate 131 may indicate which measuring device has produced the measurement re-

sults, in which units the measurement result is presented, and what is the measurement accuracy of the result.

In an embodiment of the invention the at least one memory 204 and the computer program code 205 are further configured with the at least one processor 202 to cause the measuring device 200A to protect communication with an external third party. By means of the data security module 100 the measurement results may for example be protected from external observers, for example by using a cryptographically protected connection between the data security module 100 and an external server and/or by using a cryptographic key which may be protected using the key storage 110 in a way that enables trusted third parties to access the measurement results but prevents the access of others to their content. This function may protect different parts of the measurement results, such as only numerical values, in addition to the numerical values also other information, or for example all information of the measurement results including the signatures. This function may be implemented using for example public or secret key cryptographic methods.

The data security module 100 may be provided such that it is directly integrated into a digital business platform, which enables the connection of an IoT measuring device to an open network and the selling of data in a data market. This may mean, for example, that the measurements signed with the data security module 100 are protected such that they may only be utilized by a licensed party or parties and that at least the licensed parties may verify the authenticity of the signature.

An example of the digital business platform is a business platform, i.e. a marketplace by means of which the businesses providing measurement results may offer for utilization and third parties may utilize the

generated measurement data and/or respective metadata, such as place and time, and for example information on the measurement calibration of the device, such as measurement accuracy, measurement unit and the performer of the calibration.

An advantageous embodiment of the invention may include a data security module implemented as a microcircuit, and a combination of so-called cloud services, one or more blockchains and one or more distributed databases. In this embodiment, the cloud services, block chain(s) and database or databases form a technical platform on which the above-mentioned digital business platform is implemented.

Such microcircuit implementation may be based on a so-called SoC (system on chip) technology in which on the same semiconductor chip several different hardware functions are integrated to enable the storage and execution of software utilizing them, and/or a so-called SiP (system in package) technology in which in the same package there are several semiconductor chips coupled partly to each other and partly to the outside world.

The distributed database used or a plurality of such databases may be implemented with a so-called distributed ledger technology (DLT). The DLT used may be for example Hyperledger Indy or Corda R3. The blockchain or DLT used may include a so-called smart contract function.

Combining the blockchains and databases implemented with DLT in the system into a technical platform and/or to implement the digital business platform may be based on so-called interledger methods. The interledger methods may be fully or partly based on so-called HTLA (hashed time lock agreement) protocols and/or algorithms. Such HTLA or other interledger method may be based on a component or function implemented with the above-described microcircuit. Such function may for example be reliable measurement of time (e.g. the real-

time clock 150), an accelerator of a cryptographic function (e.g. the signing function 120) and/or a secure cryptographic key storage and use function (e.g. the key storage 110 and/or the certificate storage 130).

One or some of the distributed databases or blockchains used may be integrated and partly (or fully) implemented with a microcircuit. Such microcircuit implementation may be implemented partly (or fully) as a hardware, i.e. semiconductor implementation. Such hardware implementation may include an accelerator suitable for implementing a so-called proof of work (PoW) or other corresponding (proof of stake, proof of elapsed time, etc.) method. The accelerator may be for example hardware implementation of the digital hash function. The hash function used may be for example SHA-256 or another digital hash function generally used in interledger or distributed database implementations.

Fig. 2C is a block diagram of another measuring device 200B according to the invention. In the example of Fig. 2B, the feature that the measuring device 200B is arranged in connection with the data security module 100 means that the data security module 100 is implemented as an external module with respect to the measuring device 200B and connected to the measuring device 200B in such a way that the data security module 100 and the measuring device 200B are able to communicate with each other. In other features the measuring device 200B corresponds to the measuring device 200A of Fig. 2B and therefore the measuring instrument 201, the processor 202, the memory 204, the computer program code 205, their operation and interaction with the data security module 100 are not described again in this connection.

Fig. 3A presents an example flow diagram of a method 500A for certification of a measurement result of the measuring device 200A, 200B.

Operation 501 comprises taking under processing, by the measuring device 200A, 200B, a measurement result produced using the measuring device 200A, 200B.

Operation 502 comprises associating, by the measuring device 200A, 200B, the digital calibration certificate 131 with the measurement result taken under processing, the digital calibration certificate associated with the public key 132 corresponding to the secret key 111 stored in the key storage 110 of the data security module 100 arranged in connection with the measuring device 200A, 200B.

Operation 503 comprises digitally signing, by the measuring device 200A, 200B, the associated measurement result using the signing function 120 of the data security module 100 and the secret key 111 stored in the key storage 110.

Optional operation 504 comprises generating, by the measuring device 200A, 200B, a hash of the signed measurement result, and operation 505 comprises storing, by the measuring device 200A, 200B, the generated hash in a blockchain.

Optional operation 506A comprises generating, by the measuring device 200A, 200B, a timestamp for the signed measurement result using the real-time clock 150.

The method 500A may be performed by the measuring devices 200A, 200B of Fig. 2B, 2C. The additional features of the method 500A result directly from the functions and parameters of the devices 200A, 200B, and are therefore not repeated here. The method 500A may be performed by one or more computer programs. The operations of the method 500A may be performed in an order differing from that presented in the example of Fig. 3A. For example, operation 506A of generating a timestamp may alternatively be performed for example before operation 503 of digital signing.

Fig. 3B presents an example flow diagram of a method 500B for certification of a measurement result of the measuring device 200A, 200B.

The method 500B comprises optional operation 506B of generating, by the measuring device, a timestamp for the signed measurement result using eIDAS (Electronic Identification, Authentication and Trust Services). In other features the method 500B corresponds to the method 500A of Fig. 3A and therefore operations 501-505 are not described again in this connection.

The method 500B may be performed by the measuring devices 200A, 200B of Fig. 2B, 2C. The additional features of the method 500B result directly from the functions and parameters of the devices 200A, 200B, and are therefore not repeated here. The method 500B may be performed by one or more computer programs. The operations of the method 500B may be performed in an order differing from that presented in the example of Fig. 3B. For example, operation 506B of generating a timestamp may alternatively be performed for example before operation 503 of digital signing.

The example embodiments may include, for example, any suitable measuring devices and equivalent devices capable of performing the processes of the example embodiments. The devices and subsystems of the example embodiments may communicate with each other using any suitable protocol and may be implemented using one or more programmed measuring systems or devices.

One or more interface mechanisms may be used with the example embodiments, including for example Internet connection, telecommunication in any suitable form (e.g. voice, modem, etc.), wireless communication media, and the like. The communication networks or connections used may include for example one or more satellite communication networks, wireless communication networks, cellular communication networks, 3G communi-

cation networks, 4G communication networks, 5G communication networks, public switched telephone network, packet data networks, Internet, intranet networks, a combination of some of them etc.

It is to be understood that the example embodiments are examples only, because many modifications of the specific hardware used for implementing the example embodiments are possible, as will be appreciated by persons skilled in the art. For example, the functionality of one or more components of the example embodiments may be implemented by way of hardware and/or software.

The example embodiments may store information related to the different processes described in this disclosure. Such information may be stored in one or more memories such as, for example, a hard disk, an optical disk, a magneto-optical disk, a RAM, etc. The information used for implementing the example embodiments of the present invention may be stored in one or more databases. The databases may be organized using data structures (e.g. records, arrays, tables, fields, graphs, trees, lists, etc.) included in one or more of the memories or storage devices listed herein. The processes described for the example embodiments may include the relevant data structures for storing the data collected and/or generated by the processes of the devices and subsystems of the example embodiments in one or more databases.

The example embodiments may be implemented fully or partly using one or more general-purpose processors, microprocessors, DSPs, microcontrollers, etc., which are programmed according to the teachings of the example embodiments of the present invention, as persons skilled in the art would understand. The average programmer may easily produce the relevant software on the basis of the teachings of the example embodiments, as persons skilled in the software arts would understand. In addition, the example embodiments may be implemented

with application-specific integrated circuits or by combining a relevant network of traditional component circuits, as is understood by persons skilled in the electronic arts. Thus, the example embodiments are not limited to any specific combination of hardware and/or software.

Stored on any computer-readable medium or their combination, the example embodiments of the present invention may comprise software for controlling the components of the example embodiments, running the components of the example embodiments, enabling interaction of the components of the example embodiments with a human user etc. This type of software may include, but is not limited to, device drivers, firmware, operating systems, software development tools, application software, etc. The computer-readable media may further include the computer program product according to an embodiment of the present invention for executing the processes to be performed to implement the invention fully or partly (if the processing is distributed). The computer code devices of the example embodiments of the present invention may include any suitable interpretable or executable code mechanisms, including but not limited to scripts, interpretable programs, dynamic link libraries, Java classes and applets, fully executable programs etc. In addition, parts of the processing of the example embodiments of the present invention may be distributed to improve performance, reliability, costs etc.

As stated above, the components of the example embodiments may include a computer-readable medium or memory for storing the instructions programmed according to the teachings of the present invention and for storing the data structures, arrays, records and/or other data described in this disclosure. The computer-readable medium may comprise any suitable medium which participates in arranging instructions for being executed by a processor. This type of medium may take many different

forms, including but not limited to a non-volatile or non-transitory storage medium, a volatile or transitory storage medium, etc. A non-volatile storage medium may comprise for example optical or magnetic disks, etc. A volatile storage medium may comprise for example dynamic memories etc. General forms of the computer-readable medium may include for example a floppy disk, a hard disk or any other suitable medium from which a computer may read.

The invention is not limited only to the above-described examples of its embodiments; instead, many modifications are possible within the scope of the inventive idea defined by the claims.

CLAIMS

1. A data security module (100), comprising:

a key storage (110), configured to store a cryptographic key in a protected manner, such that said cryptographic key is usable internally in the data security module (100) without being accessible from outside of the data security module (100); and

a signing function (120), configured to perform digital signing using the cryptographic key stored in the key storage (110),

c h a r a c t e r i z e d in that the data security module (100) further comprises:

a certificate storage (130), configured to store at least a part of a digital calibration certificate (131) associated with a measuring device (200A, 200B) associated with the data security module (100), such that said at least part of the digital calibration certificate (131) is accessible from outside of the data security module (100),

wherein the cryptographic key stored in the key storage (110) is a secret key (111) of a public key cryptography key pair associated with said measuring device (200A, 200B), and the at least part of the digital calibration certificate (131) stored in the certificate storage (130) is associated with a public key (132) corresponding to said secret key (111).

2. The data security module (100) according to claim 1, further comprising:

a PUF (physically unclonable function) (140) for generating said secret key (111) during runtime.

3. The data security module (100) according to claim 1 or 2, further comprising:

a real-time clock (150).

4. The data security module (100) according to any one of claims 1-3, further comprising:

a communication function (160) for external communication of the data security module (100).

5. The data security module (100) according to any one of claims 1-4, wherein the protection of the key storage (110) is implemented on a hardware level.

6. The data security module (100) according to any one of claims 1-5, wherein the signing function (120) is implemented at least partly on a hardware level.

7. The data security module (100) according to any one of claims 1-6, wherein the at least part of the digital calibration certificate (131) stored in the certificate storage (130) comprises said public key (132).

8. The data security module (100) according to any one of claims 1-6, wherein the at least part of the digital calibration certificate (131) stored in the certificate storage (130) comprises identity information associated with said public key (132).

9. A measuring device (200A, 200B) arranged in connection with the data security module (100) according to any one of claims 1-8 and comprising:

a measuring instrument (201);

at least one processor (202); and

at least one memory (204) comprising computer program code (205), c h a r a c t e r i z e d in that the at least one memory (204) and the computer program code (205) are configured to, with the at least one processor (202), cause the measuring device (200A, 200B) to:

take under processing a measurement result produced using the measuring instrument (201);

associate a digital calibration certificate (131) associated with a public key (132) corresponding to a secret key (111) stored in a key storage (110) of the data security module (100) with the measurement result taken under processing; and

digitally sign the associated measurement result using a signing function (120) of the data security module (100) and the secret key (111) stored in the key storage (110).

10. The measuring device (200A, 200B) according to claim 9, wherein the at least one memory (204) and the computer program code (205) are further configured with the at least one processor (202) to cause the measuring device (200A, 200B) to:

perform the association of the digital calibration certificate (131) with the measurement result taken under processing by generating a hash of the digital calibration certificate (131) and by including the generated hash in the measurement result taken under processing.

11. The measuring device (200A, 200B) according to claim 9 or 10, wherein the at least one memory (204) and the computer program code (205) are further configured with the at least one processor (202) to cause the measuring device (200A, 200B) to:

generate a hash of the signed measurement result; and

store the generated hash in a blockchain.

12. The measuring device (200A, 200B) according to any one of claims 9-11, wherein the data security module (100) comprises a real-time clock (150) and the at least one memory (204) and the computer program code (205) are further configured with the at least one processor (202) to cause the measuring device (200A, 200B) to:

generate a timestamp for the signed measurement result using the real-time clock (150).

13. The measuring device (200A, 200B) according to any one of claims 9-11, wherein the at least one memory (204) and the computer program code (205) are further configured with the at least one processor (202) to cause the measuring device (200A, 200B) to:

generate a timestamp for the signed measurement result using eIDAS (Electronic Identification, Authentication and Trust Services).

14. The measuring device (200A, 200B) according to any one of claims 9-13, wherein the at least one memory (204) and the computer program code (205) are further configured with the at least one processor (202) to cause the measuring device (200A, 200B) to:

protect communication with an external third party.

15. A method (500A, 500B) of certification of a measurement result of a measuring device, characterized in that the method (500A, 500B) comprises steps of:

taking (501) under processing, by the measuring device, a measurement result produced using the measuring device;

associating (502), by the measuring device, a digital calibration certificate with the measurement result taken under processing, the digital calibration certificate associated with a public key corresponding to a secret key stored in a key storage of the data security module according to any one of claims 1-8 arranged in connection with the measuring device; and

digitally signing (503), by the measuring device, the associated measurement result using a signing function of the data security module and the secret key stored in the key storage.

16. The method (500A, 500B) according to claim 15, wherein the association of the digital calibration certificate with the measurement result taken under processing is performed by generating a hash of the digital calibration certificate and by including the generated hash in the measurement result taken under processing.

17. The method (500A, 500B) according to claim 15 or 16, further comprising:

generating (504), by the measuring device, a hash of the signed measurement result; and

storing (505), by the measuring device, the generated hash in a blockchain.

18. The method (500A) according to any one of claims 15-17, wherein the data security module comprises a real-time clock and the method (500A) further comprises:

generating (506A), by the measuring device, a timestamp for the signed measurement result using the real-time clock.

19. The method (500B) according to any one of claims 15-17, further comprising:

generating (506B), by the measuring device, a timestamp for the signed measurement result using eIDAS (Electronic Identification, Authentication and Trust Services).

20. A computer program product comprising at least one computer-readable storage medium which comprises a set of instructions which, when executed by one or more processors (202), cause a measuring device (200) to perform the method according to any one of claims 15-19.

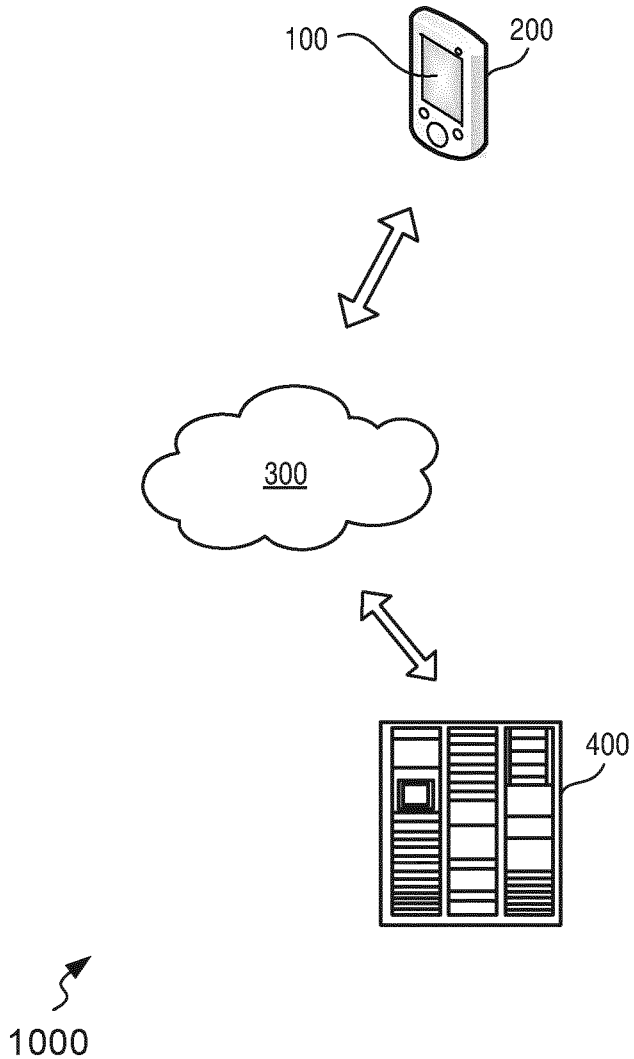

FIG. 1

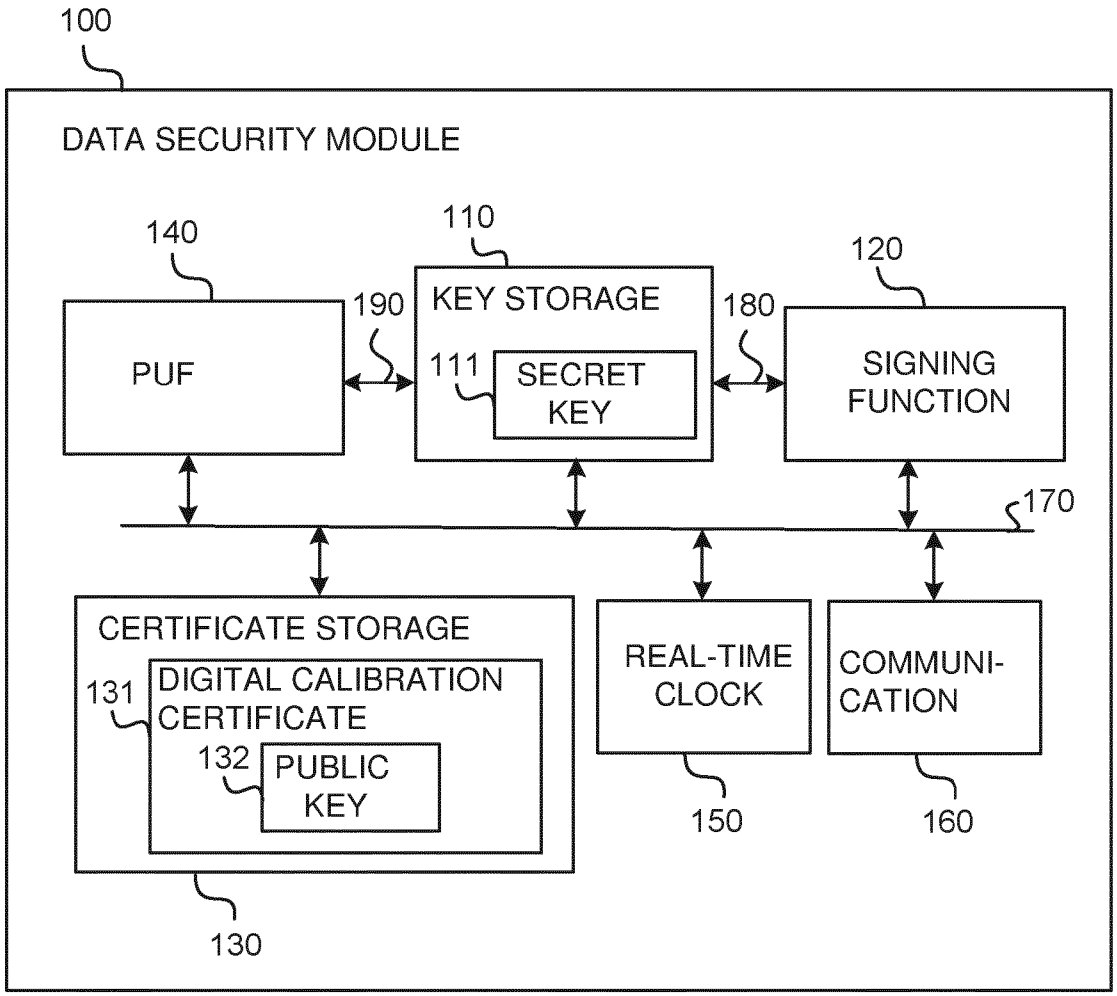
100
DATA SECURITY MODULE
140
PUF
110
KEY STORAGE
111
SECRET KEY
190
180
120
SIGNING FUNCTION
170
CERTIFICATE STORAGE
131
DIGITAL CALIBRATION CERTIFICATE
132
PUBLIC KEY
130
REAL-TIME CLOCK
150
COMMUNI-CATION
160

FIG. 2A

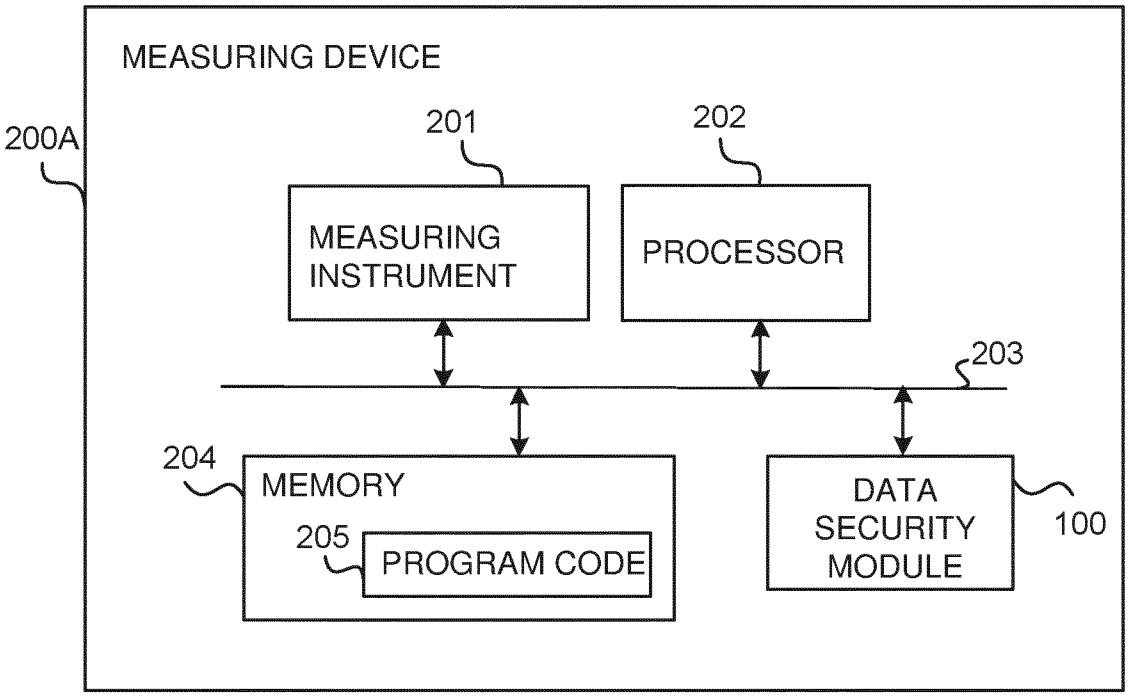
MEASURING DEVICE
200A
201
202
MEASURING INSTRUMENT
PROCESSOR
203
204
MEMORY
205
PROGRAM CODE
DATA SECURITY MODULE
100

FIG. 2B

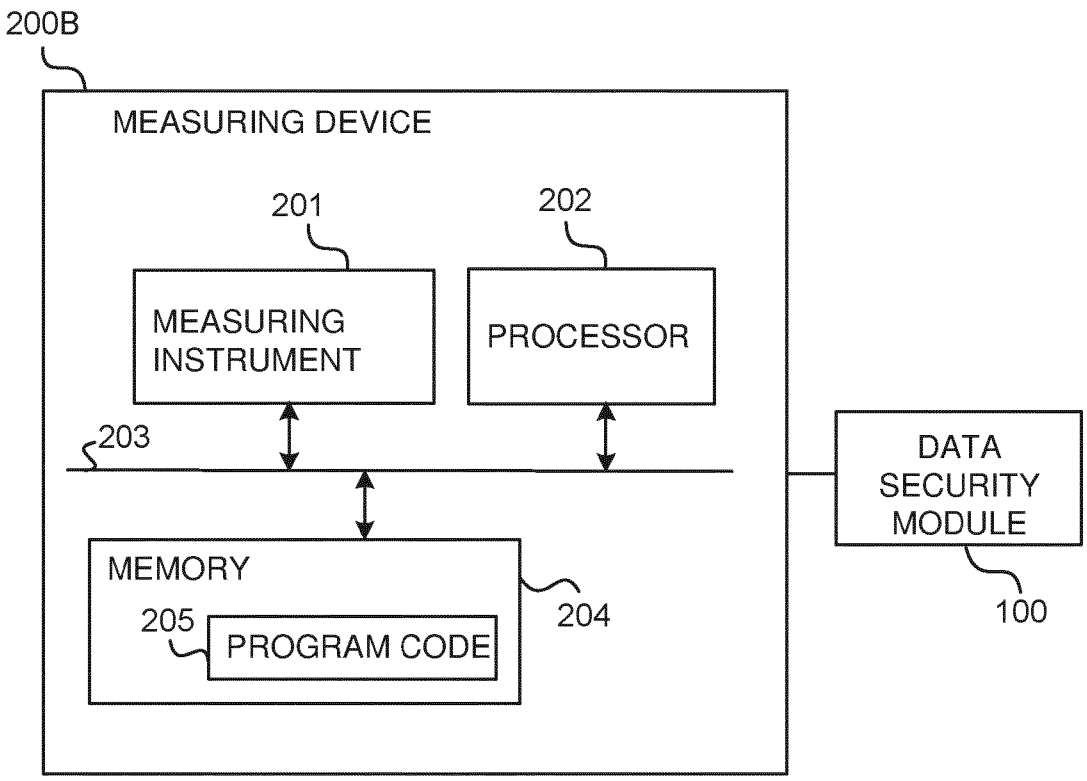
200B
MEASURING DEVICE
201
202
MEASURING INSTRUMENT
PROCESSOR
203
DATA SECURITY MODULE
MEMORY
205
PROGRAM CODE
204
100

FIG. 2C

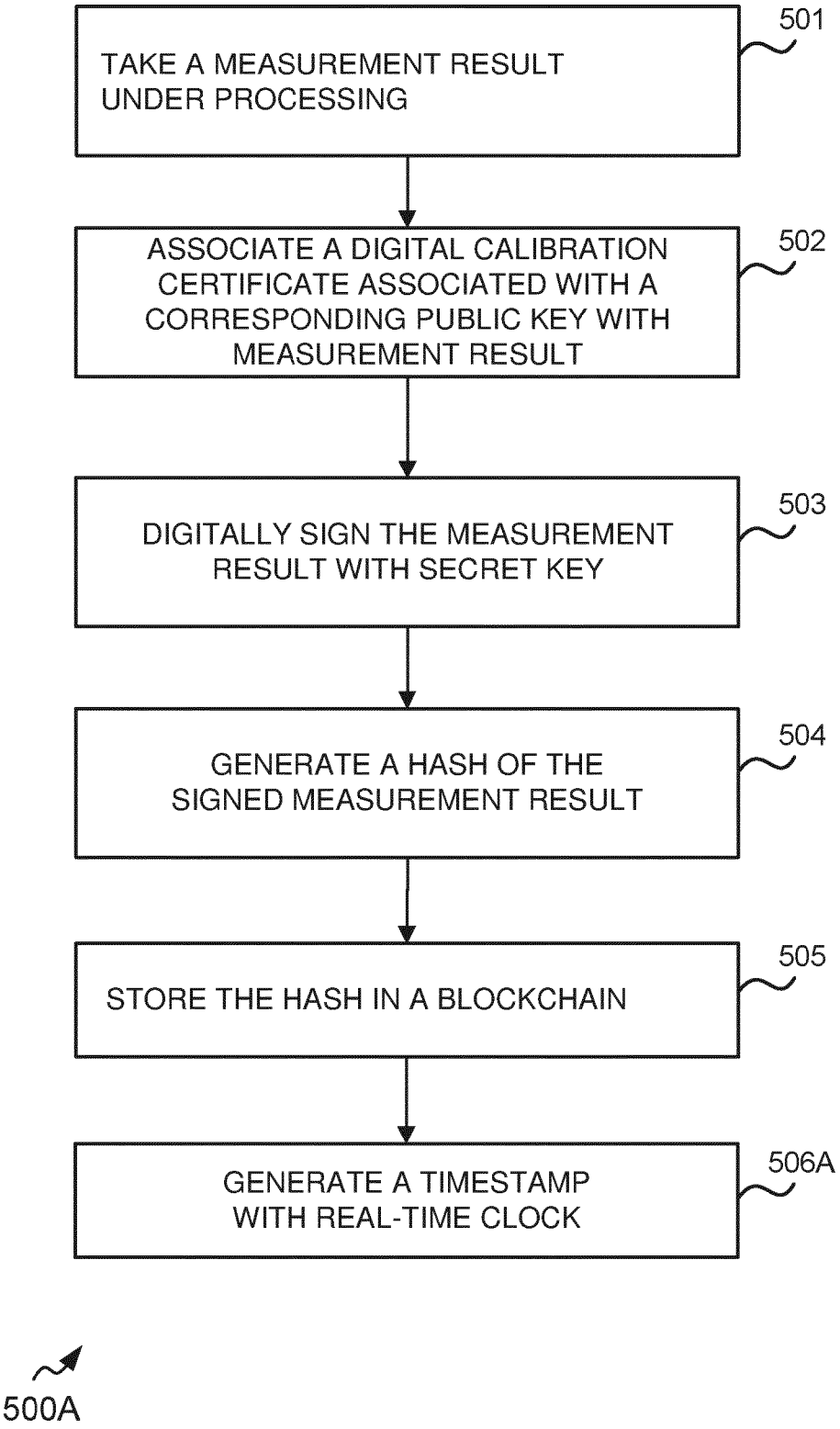
TAKE A MEASUREMENT RESULT UNDER PROCESSING
501
ASSOCIATE A DIGITAL CALIBRATION CERTIFICATE ASSOCIATED WITH A CORRESPONDING PUBLIC KEY WITH MEASUREMENT RESULT
502
DIGITALLY SIGN THE MEASUREMENT RESULT WITH SECRET KEY
503
GENERATE A HASH OF THE SIGNED MEASUREMENT RESULT
504
STORE THE HASH IN A BLOCKCHAIN
505
GENERATE A TIMESTAMP WITH REAL-TIME CLOCK
506A
500A

FIG. 3A

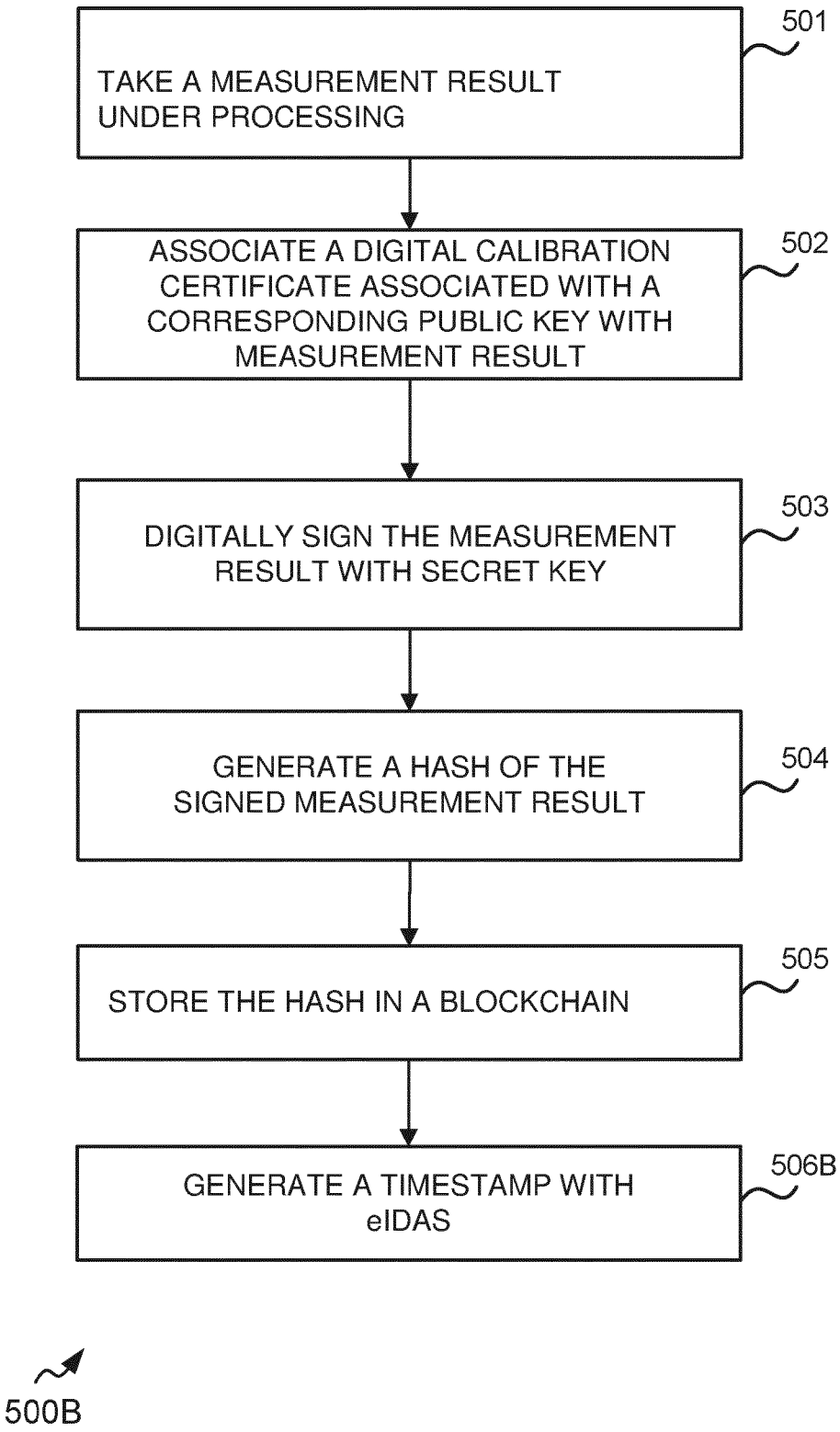
TAKE A MEASUREMENT RESULT UNDER PROCESSING
501
ASSOCIATE A DIGITAL CALIBRATION CERTIFICATE ASSOCIATED WITH A CORRESPONDING PUBLIC KEY WITH MEASUREMENT RESULT
502
DIGITALLY SIGN THE MEASUREMENT RESULT WITH SECRET KEY
503
GENERATE A HASH OF THE SIGNED MEASUREMENT RESULT
504
STORE THE HASH IN A BLOCKCHAIN
505
GENERATE A TIMESTAMP WITH eIDAS
506B
500B

FIG. 3B

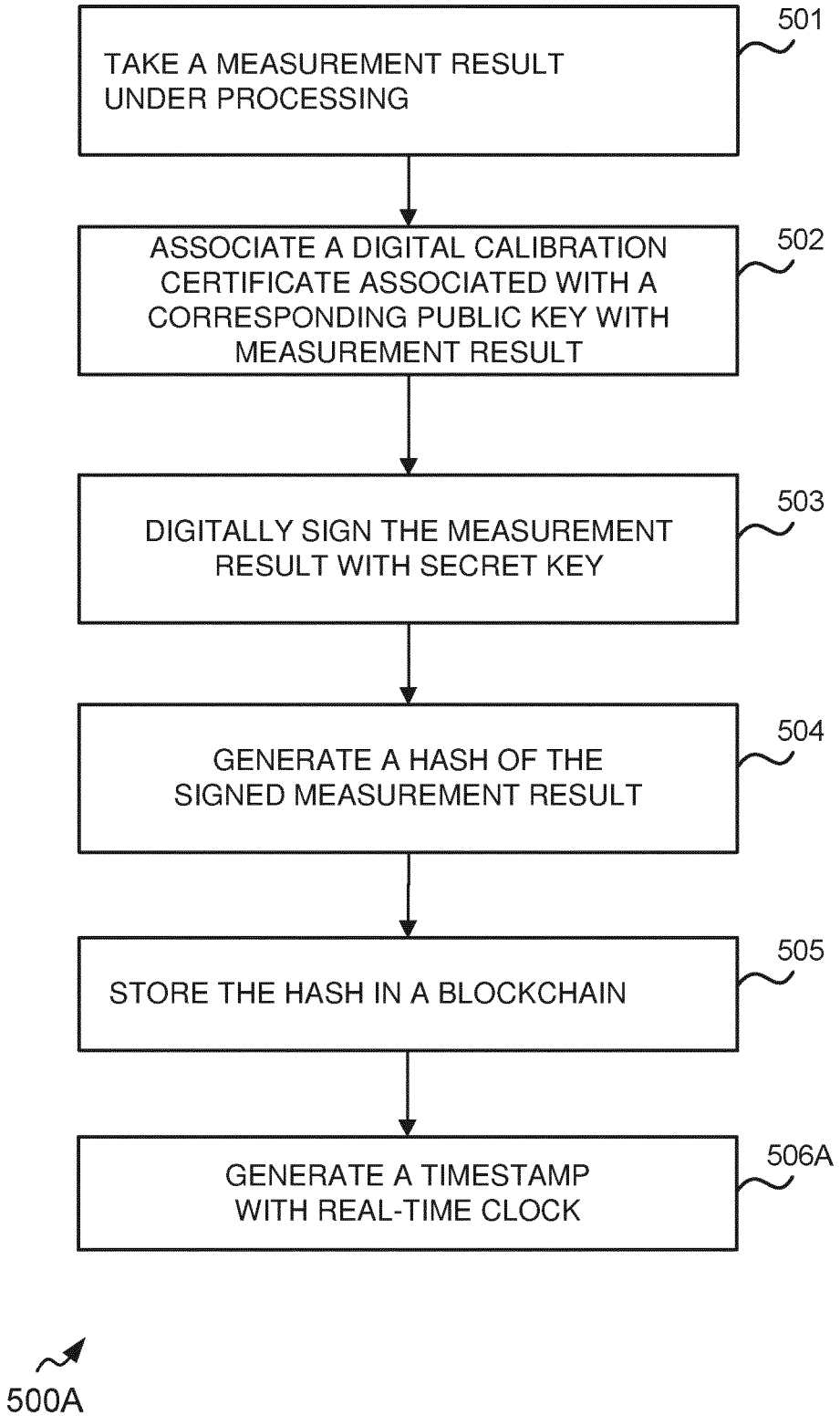
TAKE A MEASUREMENT RESULT UNDER PROCESSING
501
ASSOCIATE A DIGITAL CALIBRATION CERTIFICATE ASSOCIATED WITH A CORRESPONDING PUBLIC KEY WITH MEASUREMENT RESULT
502
DIGITALLY SIGN THE MEASUREMENT RESULT WITH SECRET KEY
503
GENERATE A HASH OF THE SIGNED MEASUREMENT RESULT
504
STORE THE HASH IN A BLOCKCHAIN
505
GENERATE A TIMESTAMP WITH REAL-TIME CLOCK
506A
500A

FIG. 3A