



(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

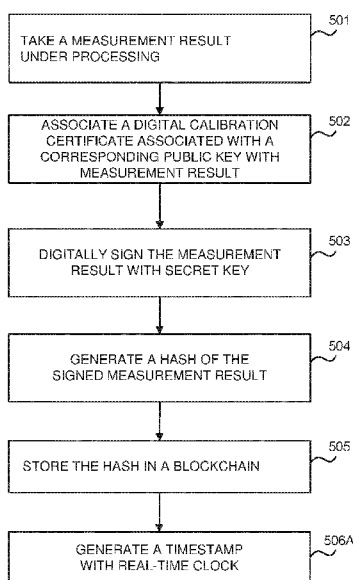
UNIVERSITY FOUNDATION SR, P.O. Box 11000, 00076 Aalto (FI).

(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



500A

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).



**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 automation 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.

5           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 pro-  
10           cessor, 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:

15           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  
20           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  
25           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 gen-  
30           erated 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  
35           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 block-chain.

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.

5           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 block-chain.

10           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.

15           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).

20           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  
25 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  
30 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  
35 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;

5 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.

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

#### **DETAILED DESCRIPTION OF THE INVENTION**

15 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  
20  
25 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  
30 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  
35 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  
5 (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  
10 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  
15 140 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  
20 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.

25 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  
30 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  
35 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.

10 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  
15 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  
25 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  
30 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  
35 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  
5 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  
10 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  
15 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 de-  
20 vices. 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  
25 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  
30 be arranged for example on a printed circuit board, such as a mother board or the like.

The measuring device 200A illustrated and de-  
scribed herein is only an example of a device which may utilize the embodiments of the invention, and it is not  
35 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:

```
5         <measurement-result-with-associated-calibra-
           tion-certificate>
           <measurement-result>...</measurement-result>
           <associated-calibration-certificate>
10        <calibration-certificate-identifier>...</cal-
           ibration-certificate-identifier>
           <calibration-certificate-finger-
           print>...</calibration-certificate-fingerprint>
           </associated-calibration-certificate>
           </measurement-result-with-associated-calibra-
15        tion-certificate>
```

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

```
20        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
25        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:

```
30        <signed-measurement-result>
           <measurement-result-with-associated-calibra-
           tion-certificate>
           <measurement-result>...</measurement-result>
           <associated-calibration-certificate>
35        <calibration-certificate-identifier>...</cal-
           ibration-certificate-identifier>
```

```

    <calibration-certificate-finger-
print>...</calibration-certificate-fingerprint>
    </associated-calibration-certificate>
  </measurement-result-with-associated-calibra-
5     tion-certificate>
    <digital-signature>...</digital-signature>
    </signed-measurement-result>

```

10 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  
15 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  
20 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  
25 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  
30 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  
35 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  
5 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  
10 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  
15 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 ex-  
20 ample 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  
25 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  
30 100 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  
35 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).

5           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  
10           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.  
15           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  
20           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  
25           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  
30           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  
35           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.

5           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  
10 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  
15 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  
20 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  
25 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  
30 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  
35 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.

5           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  
10 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  
15 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  
20 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  
25 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.,  
30 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  
35 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  
5 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.

10           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),  
characterized 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  
5 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  
10 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  
15 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:

20 a measuring instrument (201);  
at least one processor (202); and  
at least one memory (204) comprising computer program code (205), characterized in that the at least one memory (204) and the computer program code  
25 (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);

30 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

35 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  
5 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  
10 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  
15 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  
20 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  
30 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  
35 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)  
5 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;

15 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

20 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:

35 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:

5           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:

10           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.

20

1 / 5

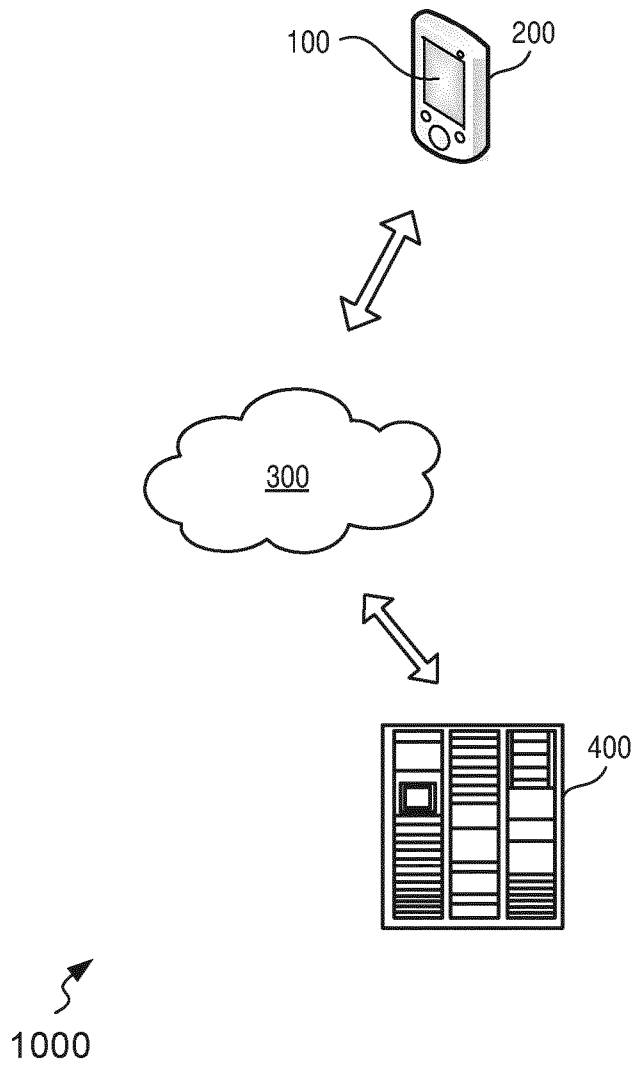


FIG. 1

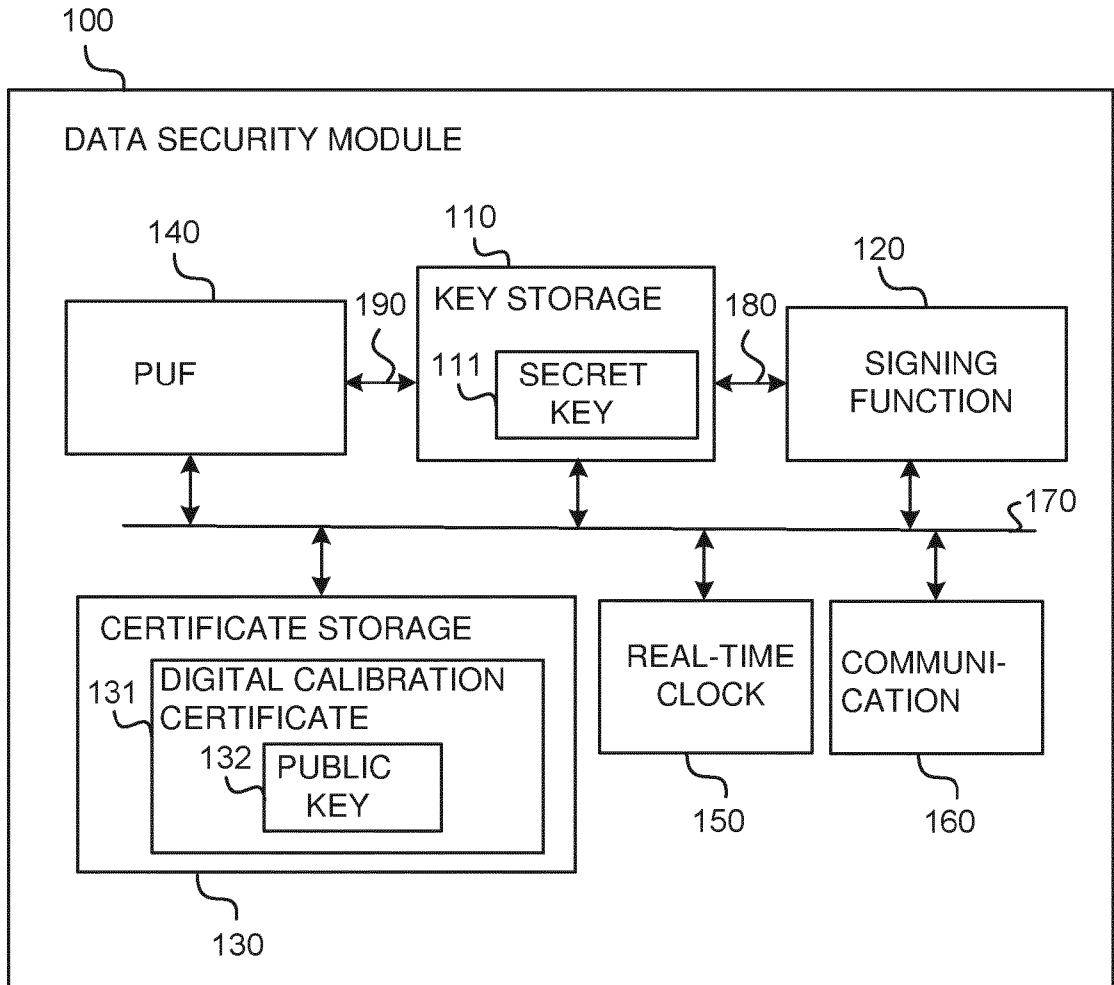


FIG. 2A

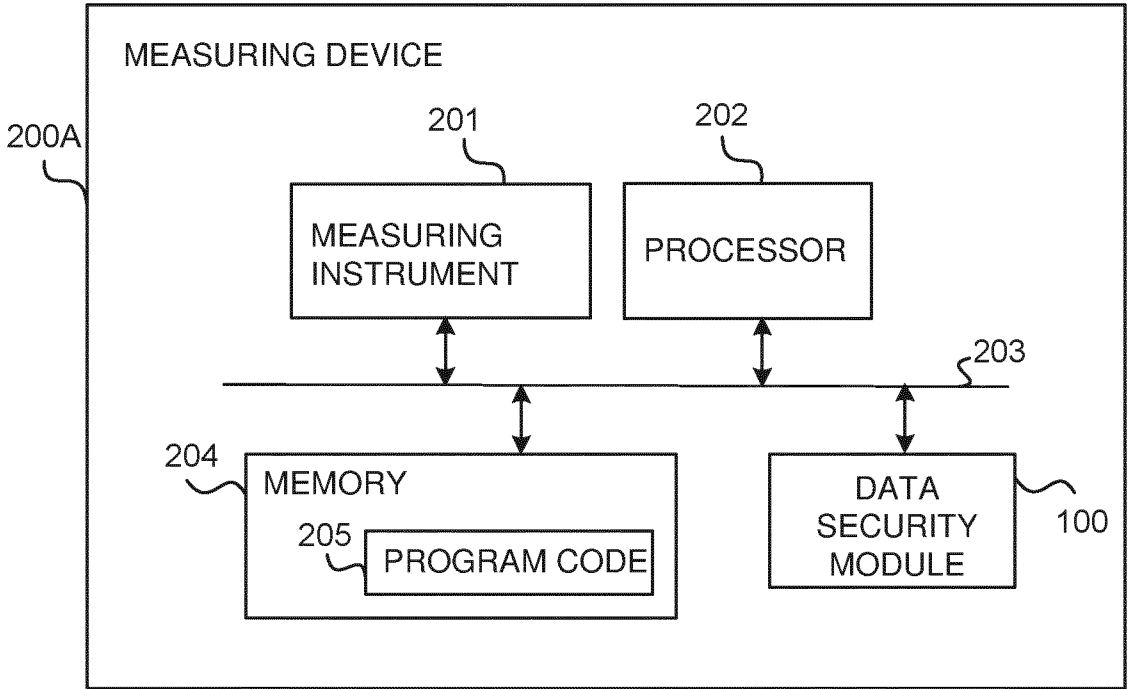


FIG. 2B

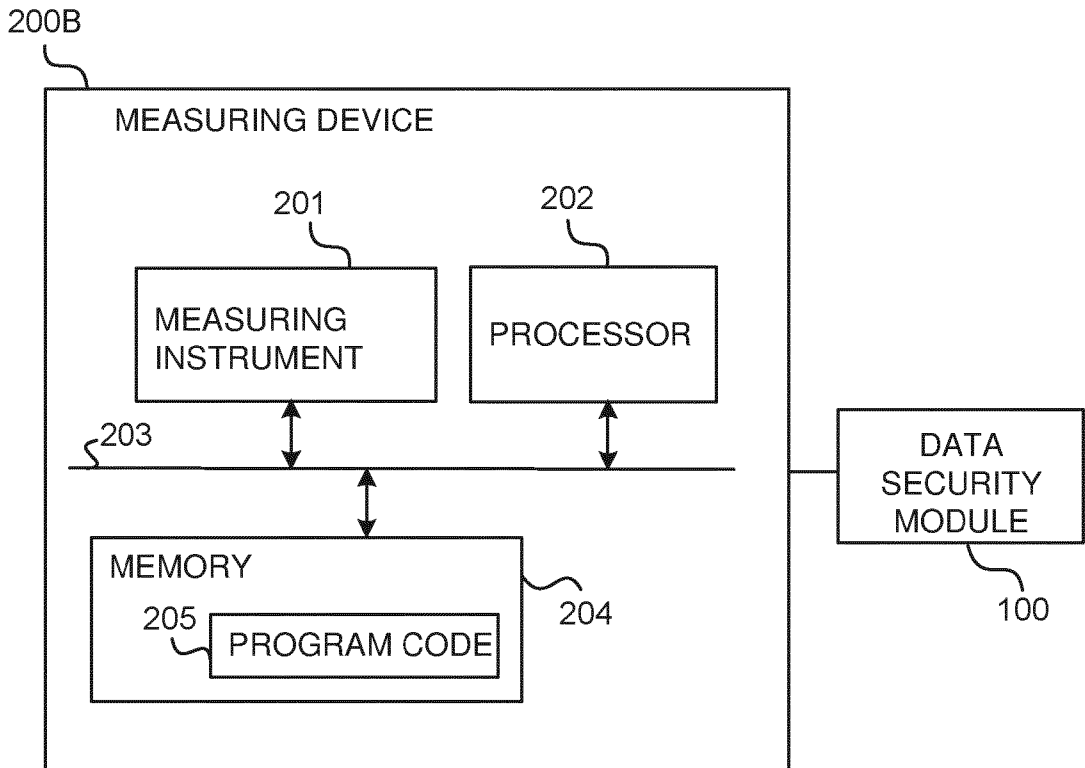


FIG. 2C

4 / 5

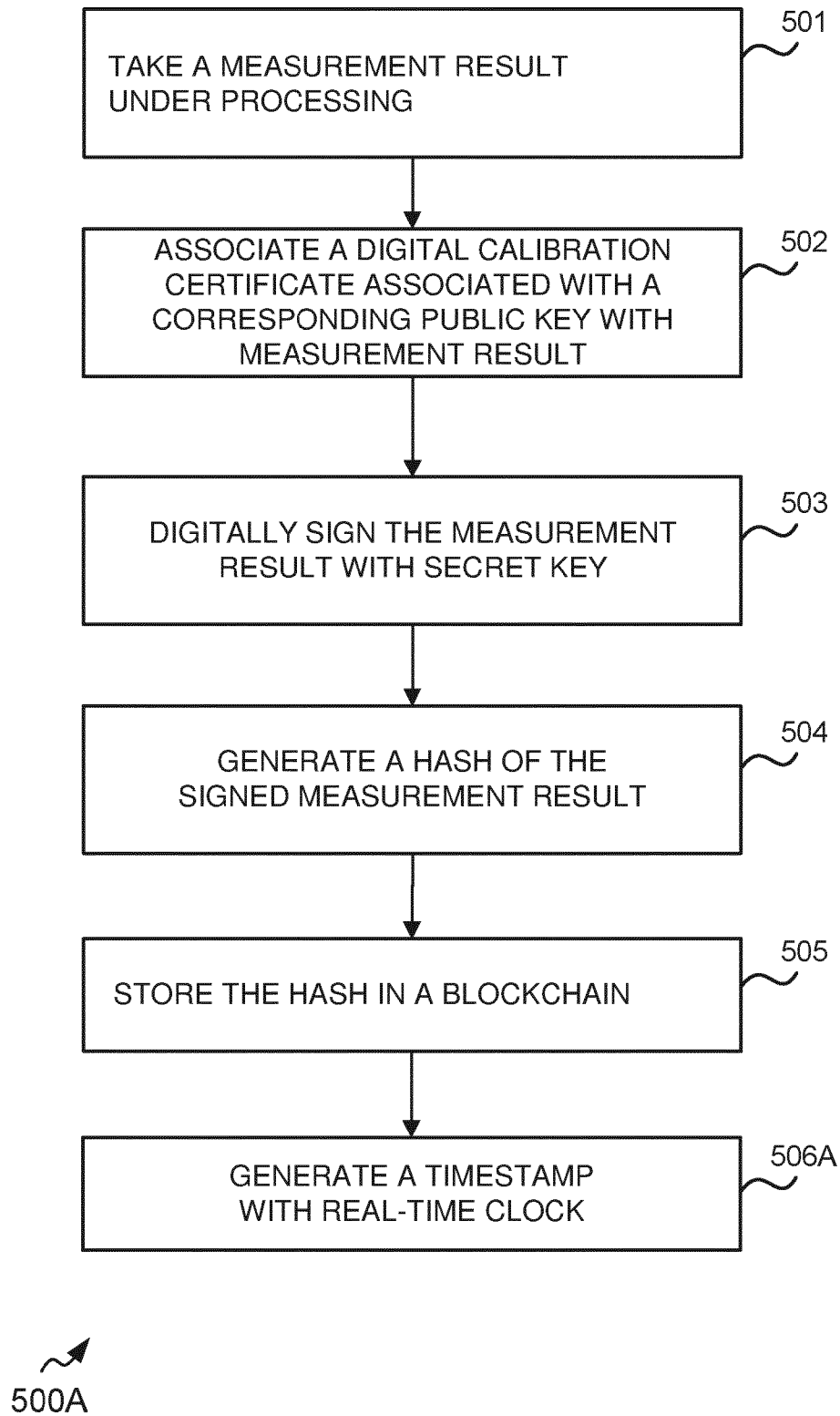
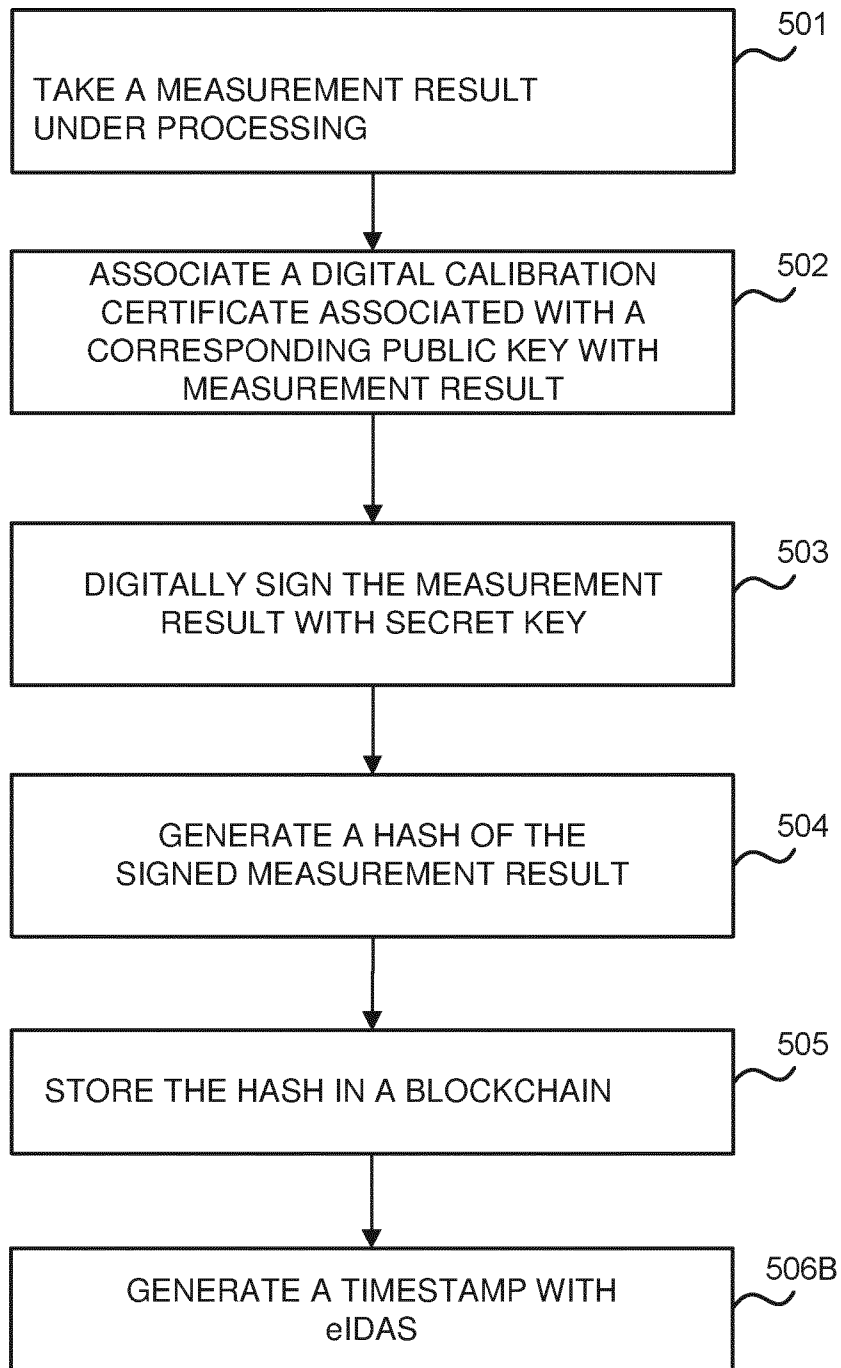


FIG. 3A

5 / 5



500B

FIG. 3B

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2020/050312

<b>A. CLASSIFICATION OF SUBJECT MATTER</b>		
See extra sheet		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b>		
Minimum documentation searched (classification system followed by classification symbols)		
IPC: G01D, G06F, H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
FI, SE, NO, DK		
Electronic data base consulted during the international search (name of data base, and, where practicable, search terms used)		
EPODOC, EPO-Internal full-text databases, Full-text translation databases from Asian languages, WPIAP, XPAIP, XPESP, XPI3E, XPIEE, XPIOP, XPIPCOM, XPMISC, XPOAC, XPRD, XPSPRNG, XPTK, COMPDX, INSPEC, TDB		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014298044 A1 (WALKER JAY S [US] et al.) 02 October 2014 (02.10.2014) Abstract; Fig. 1; paragraphs [0014]-[0015], [0031]-[0033], [0035], [0037]-[0038], [0063], [0065], [0068], [0081]	1-20
X	US 2014025944 A1 (MALETSKY KERRY [US] et al.) 23 January 2014 (23.01.2014) Abstract; Fig. 2; claims 1, 7-8, 11, 13-14; paragraph [0070]	1-20
A	US 2019113492 A1 (JENSEN JESPER [AE]) 18 April 2019 (18.04.2019) Paragraph [0017]	1-20
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "D" document cited by the applicant in the international application "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 22 July 2020 (22.07.2020)		Date of mailing of the international search report 27 July 2020 (27.07.2020)
Name and mailing address of the ISA/FI Finnish Patent and Registration Office FI-00091 PRH, FINLAND Facsimile No. +358 29 509 5328		Authorized officer Vesa-Matti Louekoski Telephone No. +358 29 509 5000

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2020/050312

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>HACKEL, SG et al. "The Digital Calibration Certificate". PTB-Mitteilungen [online], 2017 [retrieved on 2020-07-21], Vol. 127, Iss. 4, pp. 75-81. Retrieved from the Internet: <a href="https://oar.ptb.de/resources/show/10.7795/310.20170403">https://oar.ptb.de/resources/show/10.7795/310.20170403</a> DOI: 10.7795/310.20170403 Whole document</p>	1-20

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

US 2014298044 A1	02/10/2014	AU 6877698 A	11/11/1998
		AU 721809 B2	13/07/2000
		AU 3812097 A	10/02/1998
		AU 724040 B2	07/09/2000
		AU 4247997 A	26/03/1998
		AU 733969 B2	31/05/2001
		AU 9105798 A	16/03/1999
		AU 745406 B2	21/03/2002
		AU 3437002 A	27/06/2002
		AU 775975 B2	19/08/2004
		AU 1564702 A	11/04/2002
		AU 776323 B2	02/09/2004
		AU 1072199 A	03/05/1999
		AU 1081997 A	11/06/1997
		AU 1094700 A	26/04/2000
		AU 1097600 A	31/07/2000
		AU 1305399 A	24/05/1999
		AU 1357601 A	30/05/2001
		AU 1458400 A	12/07/2000
		AU 1841100 A	26/06/2000
		AU 1931400 A	26/06/2000
		AU 2039200 A	26/06/2000
		AU 2353400 A	19/06/2000
		AU 2444697 A	29/10/1997
		AU 2459599 A	09/08/1999
		AU 2712500 A	31/07/2000
		AU 2934697 A	12/11/1997
		AU 3092501 A	24/07/2001
		AU 3234500 A	04/09/2000
		AU 4026500 A	23/10/2000
		AU 4082699 A	13/12/1999
		AU 4087099 A	05/01/2000
		AU 4695499 A	05/01/2000
		AU 4788401 A	15/10/2001
		AU 4822799 A	05/01/2000
		AU 4931301 A	03/10/2001
		AU 4995900 A	09/01/2001
		AU 5135400 A	22/01/2001
		AU 5208999 A	01/02/2000
		AU 5313499 A	24/01/2000
		AU 5397799 A	06/03/2000
		AU 5497300 A	13/02/2001
		AU 5497400 A	09/01/2001
		AU 5627700 A	09/01/2001
		AU 5628000 A	09/01/2001
		AU 5692698 A	03/07/1998

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

AU 5905299 A	31/07/2000
AU 6052900 A	09/01/2001
AU 6058699 A	26/04/2000
AU 6087900 A	30/01/2001
AU 6343500 A	13/02/2001
AU 6394499 A	26/04/2000
AU 6402396 A	05/02/1997
AU 6405396 A	05/02/1997
AU 6661198 A	29/09/1998
AU 6771498 A	20/10/1998
AU 6774600 A	12/11/2001
AU 6864498 A	20/10/1998
AU 7143298 A	19/01/1999
AU 7569500 A	18/12/2000
AU 8289698 A	08/02/1999
AU 8290198 A	08/02/1999
AU 9027998 A	16/03/1999
AU 9200098 A	16/03/1999
AU 9201598 A	16/03/1999
AU 9496398 A	13/12/1999
AU 2002256220 B2	28/07/2005
AU 2002350180 A1	03/06/2004
AU 2003221725 A1	03/11/2003
AU 2003221973 A1	03/11/2003
AU 2003221973 B2	15/02/2007
AU 2003221974 A1	03/11/2003
AU 2003221975 A1	03/11/2003
AU 2003221975 B2	09/11/2006
AU 2003222025 A1	03/11/2003
AU 2003222661 A1	03/11/2003
AU 2003224770 A1	03/11/2003
AU 2003225919 A1	03/11/2003
AU 2003228616 A1	03/11/2003
AU 2003228618 A1	03/11/2003
AU 2003228618 B2	08/02/2007
AU 2003230946 A1	03/11/2003
AU 2003231014 A1	03/11/2003
AU 2003231066 A1	03/11/2003
AU 2003234118 A1	03/11/2003
AU 2003252901 A1	11/12/2003
AU 2003261457 A1	25/02/2004
AU 2004216719 A1	16/09/2004
AU 2004216719 B2	03/04/2008
AU 2004216724 A1	16/09/2004
AU 2004216724 B2	05/06/2008
AU 2004218352 A1	16/09/2004
AU 2004244307 A1	09/12/2004

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

AU 2004244307 B2	29/05/2008
AU 2004262431 A1	10/02/2005
AU 2004262431 B2	11/12/2008
AU 2004280987 A1	21/04/2005
AU 2005228436 A1	13/10/2005
AU 2005228436 B2	04/06/2009
AU 2008207348 A1	18/09/2008
AU 2008207348 B2	09/06/2011
AU 2008216073 A1	21/08/2008
AU 2008216073 B2	01/03/2012
AU 2009212857 A1	24/09/2009
BR 9710547 A	11/01/2000
BR 9713193 A	21/12/1999
BR 9811995 A	05/09/2000
BR 9811996 A	16/01/2001
BR 9811997 A	05/09/2000
BR 9815463 A	06/11/2001
CA 2254816 A1	23/06/1999
CA 2254816 C	05/08/2003
CA 2260272 A1	29/01/1998
CA 2260272 C	01/07/2003
CA 2273176 A1	12/03/1998
CA 2277132 A1	18/06/1998
CA 2284662 A1	01/10/1998
CA 2284662 C	20/01/2004
CA 2295079 A1	21/01/1999
CA 2296557 A1	21/01/1999
CA 2297818 A1	04/03/1999
CA 2298555 A1	04/03/1999
CA 2299341 A1	04/03/1999
CA 2299342 A1	04/03/1999
CA 2308303 A1	14/05/1999
CA 2332783 A1	02/12/1999
CA 2341219 A1	24/02/2000
CA 2377887 A1	18/01/2001
CA 2530761 A1	09/12/2004
CA 2532961 A1	10/02/2005
CA 2551450 A1	07/12/2007
CN 1244270 A	09/02/2000
CN 1253644 A	17/05/2000
CN 1267381 A	20/09/2000
CN 1272928 A	08/11/2000
CN 1272929 A	08/11/2000
CN 1329731 A	02/01/2002
CN 1337027 A	20/02/2002
CN 101366056 A	11/02/2009
CN 102316943 A	11/01/2012

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

CN 102316943 B	25/03/2015
DE 69637099 D1	05/07/2007
DE 69637099 T2	13/09/2007
DE 69835338 D1	07/09/2006
DE 69835338 T2	30/11/2006
EP 0862824 A1	09/09/1998
EP 0909494 A1	21/04/1999
EP 0926865 A1	30/06/1999
EP 0926865 B1	26/07/2006
EP 0954817 A1	10/11/1999
EP 0956117 A1	17/11/1999
EP 0956117 B1	23/05/2007
EP 0956677 A1	17/11/1999
EP 0995151 A2	26/04/2000
EP 1004180 A1	31/05/2000
EP 1008122 A1	14/06/2000
EP 1009503 A1	21/06/2000
EP 1010124 A1	21/06/2000
EP 1010284 A2	21/06/2000
EP 1013025 A2	28/06/2000
EP 1016012 A2	05/07/2000
EP 1016016 A2	05/07/2000
EP 1016043 A2	05/07/2000
EP 1021228 A1	26/07/2000
EP 1023674 A2	02/08/2000
EP 1034498 A1	13/09/2000
EP 1129420 A1	05/09/2001
EP 1141810 A2	10/10/2001
EP 1151404 A2	07/11/2001
EP 1155362 A1	21/11/2001
EP 1208450 A2	29/05/2002
EP 1236133 A2	04/09/2002
EP 1269436 A2	02/01/2003
EP 1377349 A1	07/01/2004
EP 1423817 A1	02/06/2004
EP 1494768 A1	12/01/2005
EP 1494769 A1	12/01/2005
EP 1634141 A2	15/03/2006
EP 1649347 A2	26/04/2006
EP 1677881 A2	12/07/2006
EP 1758662 A2	07/03/2007
EP 1790114 A2	30/05/2007
EP 2134431 A1	23/12/2009
IL 128716 D0	31/01/2000
IL 131143 D0	28/01/2001
IL 133416 D0	30/04/2001
IL 134034 D0	30/04/2001

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

IL 134238 D0	30/04/2001
JP H11510923 A	21/09/1999
JP 3632133 B2	23/03/2005
JP 2002512714 A	23/04/2002
JP 3977873 B2	19/09/2007
JP 2007500904 A	18/01/2007
JP 4478149 B2	09/06/2010
JP 2007518147 A	05/07/2007
JP 4478154 B2	09/06/2010
JP 2001527666 A	25/12/2001
JP 4803852 B2	26/10/2011
JP 2009043290 A	26/02/2009
JP 4921447 B2	25/04/2012
JP 2000508940 A	18/07/2000
JP 2000509860 A	02/08/2000
JP 2000511672 A	05/09/2000
JP 2000514945 A	07/11/2000
JP 2001509622 A	24/07/2001
JP 2001514410 A	11/09/2001
JP 2001520419 A	30/10/2001
JP 2001526550 A	18/12/2001
JP 2002517043 A	11/06/2002
JP 2002519775 A	02/07/2002
JP 2002519776 A	02/07/2002
JP 2002519777 A	02/07/2002
JP 2002532785 A	02/10/2002
JP 2002537606 A	05/11/2002
JP 2004246918 A	02/09/2004
JP 2004510212 A	02/04/2004
JP 2006059345 A	02/03/2006
JP 2008505402 A	21/02/2008
KR 20000068469 A	25/11/2000
KR 20010005536 A	15/01/2001
KR 20010023308 A	26/03/2001
KR 20010023311 A	26/03/2001
KR 20010023312 A	26/03/2001
KR 20020003355 A	12/01/2002
KR 20020005588 A	17/01/2002
PA 00001851	24/04/2002
PA 00001852	24/04/2002
PA 00001853	24/04/2002
PA 00001854	24/04/2002
MY 165524 A	02/04/2018
RU 99121833 A	20/09/2001
SG 178788 A1	29/03/2012
RE 39817	04/09/2007
RE 43037	20/12/2011

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

US 5768382 A	16/06/1998
US 5779549 A	14/07/1998
US 5828751 A	27/10/1998
US 5871398 A	16/02/1999
US 6041308 A	21/03/2000
US 6052667 A	18/04/2000
US 6068552 A	30/05/2000
US 6093026 A	25/07/2000
US 6138105 A	24/10/2000
US 6142872 A	07/11/2000
US 6161059 A	12/12/2000
US 6203430 B1	20/03/2001
US 6206782 B1	27/03/2001
US 6223163 B1	24/04/2001
US 6224486 B1	01/05/2001
US 6230150 B1	08/05/2001
US 6244957 B1	12/06/2001
US 6289453 B1	11/09/2001
US 6293866 B1	25/09/2001
US 6298329 B1	02/10/2001
US 6298331 B1	02/10/2001
US 6312332 B1	06/11/2001
US 6317649 B1	13/11/2001
US 6317723 B1	13/11/2001
US 6319127 B1	20/11/2001
US 6324520 B1	27/11/2001
US 6328648 B1	11/12/2001
US 6330544 B1	11/12/2001
US 6330548 B1	11/12/2001
US 6332129 B1	18/12/2001
US 6334112 B1	25/12/2001
US 6334113 B1	25/12/2001
US 6336104 B1	01/01/2002
US 2001047301 A1	29/11/2001
US 6341268 B2	22/01/2002
US 6361437 B1	26/03/2002
US 6361441 B1	26/03/2002
US 6364765 B1	02/04/2002
US 6390917 B1	21/05/2002
US 6397193 B1	28/05/2002
US 6402614 B1	11/06/2002
US 6405174 B1	11/06/2002
US 6415264 B1	02/07/2002
US 6466919 B1	15/10/2002
US 6470322 B1	22/10/2002
US 6507822 B1	14/01/2003
US 6510418 B1	21/01/2003

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

US 6513014 B1	28/01/2003
US 6520856 B1	18/02/2003
US 6530835 B1	11/03/2003
US 6542874 B1	01/04/2003
US 6567787 B1	20/05/2003
US 6582310 B1	24/06/2003
US 6598024 B1	22/07/2003
US 6601036 B1	29/07/2003
US 2002169018 A1	14/11/2002
US 6607439 B2	19/08/2003
US 6616458 B1	09/09/2003
US 2002042295 A1	11/04/2002
US 6648762 B2	18/11/2003
US 2002065579 A1	30/05/2002
US 6658323 B2	02/12/2003
US 2002090987 A1	11/07/2002
US 6692353 B2	17/02/2004
US 2002151365 A1	17/10/2002
US 6712699 B2	30/03/2004
US 2002042296 A1	11/04/2002
US 6733390 B2	11/05/2004
US 6751730 B1	15/06/2004
US 6754636 B1	22/06/2004
US 2003164398 A1	04/09/2003
US 6871185 B2	22/03/2005
US 6876978 B1	05/04/2005
US 2002155879 A1	24/10/2002
US 6884167 B2	26/04/2005
US 2003220132 A1	27/11/2003
US 6887153 B2	03/05/2005
US 2003125104 A1	03/07/2003
US 6890256 B2	10/05/2005
US 2003060278 A1	27/03/2003
US 6893341 B2	17/05/2005
US 6898570 B1	24/05/2005
US 2004038723 A1	26/02/2004
US 6942570 B2	13/09/2005
US 2002151358 A1	17/10/2002
US 6969317 B2	29/11/2005
US 6970837 B1	29/11/2005
US 6980968 B1	27/12/2005
US 2005143162 A1	30/06/2005
US 7008318 B2	07/03/2006
US 2002178071 A1	28/11/2002
US 7039603 B2	02/05/2006
US 7072850 B1	04/07/2006
US 2002128057 A1	12/09/2002

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

US 7094149 B2	22/08/2006
US 2002111867 A1	15/08/2002
US 7099832 B2	29/08/2006
US 2003087695 A1	08/05/2003
US 7101282 B2	05/09/2006
US 7107228 B1	12/09/2006
US 2002147040 A1	10/10/2002
US 7140964 B2	28/11/2006
US 7162434 B1	09/01/2007
US 7179168 B1	20/02/2007
US 2002193162 A1	19/12/2002
US 7192352 B2	20/03/2007
US 2006201775 A1	14/09/2006
US 7216754 B2	15/05/2007
US 2002161653 A1	31/10/2002
US 7233912 B2	19/06/2007
US 7236942 B1	26/06/2007
US 2003211889 A1	13/11/2003
US 7241219 B2	10/07/2007
US 7249050 B1	24/07/2007
US 2003083979 A1	01/05/2003
US 7251620 B2	31/07/2007
US 7272569 B1	18/09/2007
US 2004038733 A1	26/02/2004
US 7275990 B2	02/10/2007
US 2006160601 A1	20/07/2006
US 7285045 B2	23/10/2007
US 2006246998 A1	02/11/2006
US 7303468 B2	04/12/2007
US 2006231613 A1	19/10/2006
US 7347364 B2	25/03/2008
US 2004032083 A1	19/02/2004
US 7351142 B2	01/04/2008
US 2006093142 A1	04/05/2006
US 7362862 B2	22/04/2008
US 7383200 B1	03/06/2008
US 7386508 B1	10/06/2008
US 2006211479 A1	21/09/2006
US 7387571 B2	17/06/2008
US 7390255 B2	24/06/2008
US 2003199312 A1	23/10/2003
US 7416485 B2	26/08/2008
US 7438642 B2	21/10/2008
US 2006241965 A1	26/10/2006
US 7451892 B2	18/11/2008
US 2002077969 A1	20/06/2002
US 7454381 B2	18/11/2008

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

US 2006218093 A1	28/09/2006
US 7467745 B2	23/12/2008
US 2003220133 A1	27/11/2003
US 7467999 B2	23/12/2008
US 7472074 B1	30/12/2008
US 7476153 B2	13/01/2009
US 2005170880 A1	04/08/2005
US 7479060 B2	20/01/2009
US 2005261053 A1	24/11/2005
US 7485040 B2	03/02/2009
US 7493267 B1	17/02/2009
US 2006246993 A1	02/11/2006
US 7494417 B2	24/02/2009
US 2006190335 A1	24/08/2006
US 7496523 B2	24/02/2009
US 2006235770 A1	19/10/2006
US 7499769 B2	03/03/2009
US 7503851 B2	17/03/2009
US 7516089 B1	07/04/2009
US 7523045 B1	21/04/2009
US 7524244 B2	28/04/2009
US 7542919 B1	02/06/2009
US 2006246992 A1	02/11/2006
US 7547251 B2	16/06/2009
US 2006234792 A1	19/10/2006
US 7553235 B2	30/06/2009
US 2003119579 A1	26/06/2003
US 7559838 B2	14/07/2009
US 2003228902 A1	11/12/2003
US 7563167 B2	21/07/2009
US 7587333 B1	08/09/2009
US 2005075935 A1	07/04/2005
US 7587334 B2	08/09/2009
US 2006025209 A1	02/02/2006
US 7588495 B2	15/09/2009
US 7606729 B1	20/10/2009
US 7607981 B2	27/10/2009
US 7620619 B1	17/11/2009
US 2006247824 A1	02/11/2006
US 7627496 B2	01/12/2009
US 2006240892 A1	26/10/2006
US 7637811 B2	29/12/2009
US 7641036 B2	05/01/2010
US 7643902 B2	05/01/2010
US 2006224258 A1	05/10/2006
US 7658674 B2	09/02/2010
US 7664672 B1	16/02/2010

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

US 2006242028 A1	26/10/2006
US 7689468 B2	30/03/2010
US 7711604 B1	04/05/2010
US 2006252510 A1	09/11/2006
US 7722460 B2	25/05/2010
US 7729988 B1	01/06/2010
US 7739181 B2	15/06/2010
US 7747522 B1	29/06/2010
US 7753792 B2	13/07/2010
US 2006217177 A1	28/09/2006
US 7753793 B2	13/07/2010
US 7756746 B2	13/07/2010
US 2005177402 A1	11/08/2005
US 7801751 B2	21/09/2010
US 7801762 B2	21/09/2010
US 2006172794 A1	03/08/2006
US 7806763 B2	05/10/2010
US 7818284 B1	19/10/2010
US 7821404 B2	26/10/2010
US 7826923 B2	02/11/2010
US 2006218049 A1	28/09/2006
US 7827056 B2	02/11/2010
US 7827057 B1	02/11/2010
US 7828645 B2	09/11/2010
US 7831470 B1	09/11/2010
US 2006009275 A1	12/01/2006
US 7837549 B2	23/11/2010
US 2005192086 A1	01/09/2005
US 7850522 B2	14/12/2010
US 7856379 B2	21/12/2010
US 7862416 B2	04/01/2011
US 2006035701 A1	16/02/2006
US 7862424 B2	04/01/2011
US 2006226596 A1	12/10/2006
US 7862429 B2	04/01/2011
US 2006252491 A1	09/11/2006
US 7867076 B2	11/01/2011
US 7871327 B2	18/01/2011
US 2006160599 A1	20/07/2006
US 7874906 B2	25/01/2011
US 2006079321 A1	13/04/2006
US 7874911 B2	25/01/2011
US 2004147308 A1	29/07/2004
US 7874914 B2	25/01/2011
US 2006252490 A1	09/11/2006
US 7878894 B2	01/02/2011
US 2006211475 A1	21/09/2006

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

US 7878901 B2	01/02/2011
US 2006241966 A1	26/10/2006
US 7885726 B2	08/02/2011
US 2006246999 A1	02/11/2006
US 7887405 B2	15/02/2011
US 2006232003 A1	19/10/2006
US 7887414 B2	15/02/2011
US 2006229965 A1	12/10/2006
US 7895100 B2	22/02/2011
US 2006213984 A1	28/09/2006
US 7895120 B2	22/02/2011
US 7899710 B1	01/03/2011
US 7905771 B2	15/03/2011
US 2006229127 A1	12/10/2006
US 7914374 B2	29/03/2011
US 7914375 B2	29/03/2011
US 2006252486 A1	09/11/2006
US 7914376 B2	29/03/2011
US 2006079309 A1	13/04/2006
US 7922579 B2	12/04/2011
US 2006046836 A1	02/03/2006
US 7955169 B2	07/06/2011
US 7955172 B2	07/06/2011
US 7963844 B2	21/06/2011
US 7985132 B2	26/07/2011
US 7993198 B2	09/08/2011
US 7997974 B2	16/08/2011
US 2006224467 A1	05/10/2006
US 8010417 B2	30/08/2011
US 8015059 B2	06/09/2011
US 8016658 B2	13/09/2011
US 2003220138 A1	27/11/2003
US 8021229 B2	20/09/2011
US 2006217179 A1	28/09/2006
US 8025562 B2	27/09/2011
US 2006217178 A1	28/09/2006
US 8029353 B2	04/10/2011
US 2006246985 A1	02/11/2006
US 8029362 B2	04/10/2011
US 8041667 B2	18/10/2011
US 2006252514 A1	09/11/2006
US 8062122 B2	22/11/2011
US 8068933 B2	29/11/2011
US 2004014522 A1	22/01/2004
US 8070577 B2	06/12/2011
US 8082180 B2	20/12/2011
US 8082221 B2	20/12/2011

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

US 8086653 B1	27/12/2011
US 2004106454 A1	03/06/2004
US 8087996 B2	03/01/2012
US 2006218011 A1	28/09/2006
US 8092224 B2	10/01/2012
US 8096873 B2	17/01/2012
US 8103520 B2	24/01/2012
US 8105156 B2	31/01/2012
US 2003228901 A1	11/12/2003
US 8113946 B2	14/02/2012
US 8131595 B2	06/03/2012
US 8135650 B2	13/03/2012
US 8147322 B2	03/04/2012
US 2006223629 A1	05/10/2006
US 8206210 B2	26/06/2012
US 2006252515 A1	09/11/2006
US 8210928 B2	03/07/2012
US 8224760 B2	17/07/2012
US 8262394 B2	11/09/2012
US 2006252513 A1	09/11/2006
US 8277309 B2	02/10/2012
US 2006224509 A1	05/10/2006
US 8326765 B2	04/12/2012
US 2006219717 A1	05/10/2006
US 8353752 B2	15/01/2013
US 2006040730 A1	23/02/2006
US 8360857 B2	29/01/2013
US 8388430 B2	05/03/2013
US 8480467 B2	09/07/2013
US 8548871 B2	01/10/2013
US 8549310 B2	01/10/2013
US 2006234793 A1	19/10/2006
US 8556728 B2	15/10/2013
US 2003211881 A1	13/11/2003
US 8702492 B2	22/04/2014
US 8702517 B2	22/04/2014
US 8751297 B2	10/06/2014
US 8774963 B2	08/07/2014
US 8784188 B2	22/07/2014
US 2003232640 A1	18/12/2003
US 8801517 B2	12/08/2014
US 8961296 B2	24/02/2015
US 9117224 B2	25/08/2015
US 9412218 B2	09/08/2016
US 9489800 B2	08/11/2016
US 2002123376 A1	05/09/2002
US 2002156659 A1	24/10/2002

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

US 2002161610 A1	31/10/2002
US 2002173355 A1	21/11/2002
US 2002178069 A1	28/11/2002
US 2003032476 A1	13/02/2003
US 2003055744 A1	20/03/2003
US 2003064788 A1	03/04/2003
US 2003064807 A1	03/04/2003
US 2003114217 A1	19/06/2003
US 2003177347 A1	18/09/2003
US 2003224852 A1	04/12/2003
US 2004005918 A1	08/01/2004
US 2004005919 A1	08/01/2004
US 2004015423 A1	22/01/2004
US 2004024666 A1	05/02/2004
US 2004039645 A1	26/02/2004
US 2004054593 A1	18/03/2004
US 2004127290 A1	01/07/2004
US 2005165646 A1	28/07/2005
US 2005171848 A1	04/08/2005
US 2005255921 A1	17/11/2005
US 2005261973 A1	24/11/2005
US 2006025206 A1	02/02/2006
US 2006035697 A1	16/02/2006
US 2006040725 A1	23/02/2006
US 2006043668 A1	02/03/2006
US 2006046835 A1	02/03/2006
US 2006046841 A1	02/03/2006
US 2006068872 A1	30/03/2006
US 2006068903 A1	30/03/2006
US 2006084501 A1	20/04/2006
US 2006089195 A1	27/04/2006
US 2006105836 A1	18/05/2006
US 2006105837 A1	18/05/2006
US 2006111175 A1	25/05/2006
US 2006122881 A1	08/06/2006
US 2006142078 A1	29/06/2006
US 2006195368 A1	31/08/2006
US 2006211476 A1	21/09/2006
US 2006211477 A1	21/09/2006
US 2006211478 A1	21/09/2006
US 2006211480 A1	21/09/2006
US 2006211489 A1	21/09/2006
US 2006213983 A1	28/09/2006
US 2006213985 A1	28/09/2006
US 2006217176 A1	28/09/2006
US 2006217184 A1	28/09/2006
US 2006217187 A1	28/09/2006

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

US 2006217188 A1	28/09/2006
US 2006217189 A1	28/09/2006
US 2006217190 A1	28/09/2006
US 2006217193 A1	28/09/2006
US 2006217194 A1	28/09/2006
US 2006217195 A1	28/09/2006
US 2006218050 A1	28/09/2006
US 2006218092 A1	28/09/2006
US 2006218094 A1	28/09/2006
US 2006223613 A1	05/10/2006
US 2006223636 A1	05/10/2006
US 2006224464 A1	05/10/2006
US 2006224465 A1	05/10/2006
US 2006224466 A1	05/10/2006
US 2006224506 A1	05/10/2006
US 2006224510 A1	05/10/2006
US 2006226597 A1	12/10/2006
US 2006226598 A1	12/10/2006
US 2006226599 A1	12/10/2006
US 2006229124 A1	12/10/2006
US 2006229125 A1	12/10/2006
US 2006229128 A1	12/10/2006
US 2006229953 A1	12/10/2006
US 2006229966 A1	12/10/2006
US 2006231612 A1	19/10/2006
US 2006231614 A1	19/10/2006
US 2006232004 A1	19/10/2006
US 2006235754 A1	19/10/2006
US 2006235762 A1	19/10/2006
US 2006235793 A1	19/10/2006
US 2006237281 A1	26/10/2006
US 2006237282 A1	26/10/2006
US 2006240887 A1	26/10/2006
US 2006240889 A1	26/10/2006
US 2006242036 A1	26/10/2006
US 2006246986 A1	02/11/2006
US 2006246987 A1	02/11/2006
US 2006246988 A1	02/11/2006
US 2006246994 A1	02/11/2006
US 2006247000 A1	02/11/2006
US 2006247001 A1	02/11/2006
US 2006247012 A1	02/11/2006
US 2006247013 A1	02/11/2006
US 2006247014 A1	02/11/2006
US 2006247018 A1	02/11/2006
US 2006247026 A1	02/11/2006
US 2006247030 A1	02/11/2006

**INTERNATIONAL SEARCH REPORT**  
**Information on Patent Family Members**

International application No.  
PCT/FI2020/050312

US 2006247031 A1	02/11/2006
US 2006247041 A1	02/11/2006
US 2006247042 A1	02/11/2006
US 2006247973 A1	02/11/2006
US 2006248025 A1	02/11/2006
US 2006252482 A1	09/11/2006
US 2006252489 A1	09/11/2006
US 2006252497 A1	09/11/2006
US 2006252498 A1	09/11/2006
US 2006252499 A1	09/11/2006
US 2006252502 A1	09/11/2006
US 2006252509 A1	09/11/2006
US 2006252511 A1	09/11/2006
US 2006252512 A1	09/11/2006
US 2006252516 A1	09/11/2006
US 2006252517 A1	09/11/2006
US 2006252518 A1	09/11/2006
US 2006253347 A1	09/11/2006
US 2006259318 A1	16/11/2006

---

US 2014025944 A1	23/01/2014	US 9323950 B2	26/04/2016
		DE 102013213568 A1	06/02/2014

---

US 2019113492 A1	18/04/2019	EP 3440603 A1	13/02/2019
		WO 2017176266 A1	12/10/2017

---

## CLASSIFICATION OF SUBJECT MATTER

IPC

**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)