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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 July 2017 (20.07.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/123098 A1

(51) International Patent Classification:
G06F 21/32 (2013.01) *G06K 9/00* (2006.01)

(21) International Application Number:
PCT/NO2017/050011

(22) International Filing Date:
12 January 2017 (12.01.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20160057 12 January 2016 (12.01.2016) NO

(71) Applicant: **KK88.NO AS** [NO/NO]; Idrettsveien 10, 1400 Ski (NO).

(72) Inventor: **MARTHINUSSEN, Harald**; Villaveien 10, 1400 Ski (NO).

(74) Agent: **OSLO PATENTKONTOR AS**; Holtegata 20, 0306 Oslo (NO).

(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, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

(54) **Title**: A METHOD FOR VERIFYING THE IDENTITY OF A PERSON

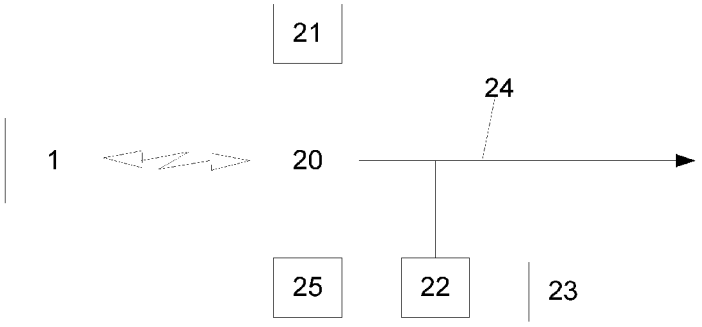

Fig. 3

(57) **Abstract**: It is described a method for generating a unique personal safe Cyber biometric identification of one user as needed by suppliers, without revealing the user's real biometric images, for use in a system for authenticating a user of a service (21, 23), the system including at least one single smart equipment (20) and a portable device (1) communicating wirelessly with each other. The equipment (20) being a PC, mobile, Pad or any single smart unit, all include storage or has access to a storage (22, 25) containing Cyber biometric image data relating to said user. The portable device (1) includes a multitude of biometric readers (3a, b, 6-12). The single smart equipment (20) is adapted to request the portable device (1) to perform and mix at least two different biometric readings on the user in order to provide a new biometric image, without revealing the real identity of the original biometric images. The new image, a Cyber biometric image, lookalike any other biometric identifications as used in the digital market, the portable device (1) being adapted to perform said at least two biometric readings on the user, combine the biometric readings forming a new mixed Cyber identity and transmit the mixed readings to the smart equipment (20), the smart equipment (20) being adapted to compare the received mixed readings with the stored Cyber biometric data, and if said received and stored biometric data agree, to allow the user access the control and use of the smart equipment as access to the online services (21, 23).

WO 2017/123098 A1

A METHOD FOR VERIFYING THE IDENTITY OF A PERSON

Field of the Invention

The present invention relates to a method for verifying the identity of a person.

Background

In today's digital society banks, governments, military, healthcare, hospitals and all companies need to protect their enormous amount of data from thieves, hackers and all unauthorized users. To connect to such a service, a user has to verify one or more personal cods as usernames, passwords, puck codes, social security numbers, birth date or biometric identification. In addition, the safety systems may have to scan your user ID cards as smart card, bankcards, company issued access cards to verify the right to connect. Apart from the strain of having to remember a lot of personal codes, the exchange of information makes the user vulnerable for personal theft, for example by onlookers gleaning the codes entered into a banking automate or used for opening a door, criminals mounting skimmers on banking automates, phishing or obtaining ID codes in other ways, or by hackers breaking into computers or smartphones, or breaking codes for using a service. It is well known that criminals have emptied bank accounts of unlucky victims and even taken over their "Cyber world" identity. There have been several attempts of solving this problem by using biometric readings for identifying a user for gaining access to an account on a computer. However, such systems require all users to be registered on beforehand, and are also only as secure as the system itself, i.e. a hacker may break the system, "get inside" and get access to the ID codes and biometric data.

Codes as username, passwords, puck codes are now substituted with biometric identification as large corporations, government as banks have decided to require your biometrical identification to secure its self against wrong users. This could have been an ideal digital world without criminals and hackers. As our digital world is full of large digital information thefts our biometric data is endangered. A person's 15 biometric unique images cannot be replaced, as codes and passwords, if stolen by hackers. If a person biometrical identity is stolen your life may be controlled by criminals or hackers. If a person loses all her/his biometric identity he/her may be digital dead forever.

International patent application WO 2014/021721, owned by the present applicant and the content of which is hereby incorporated by reference, discloses a portable system for authenticating a user trying to access a service, said device including a

CPU, ROM, RAM, at least one biometric reader, and communication means, the device being operated only by data permanently stored in the ROM, the RAM being flushed after each operating cycle. The device is adapted to read the user's private information (as smart card) and the user's private biometric data (as from fingerprints, voice, eye-iris, face shape readers). This information is mixed together with the device's unique readable production series number to secure a special coded startup of all your private equipment and help you to connect safely to your bank account, your data storage on the clouds, your government files etc. The benefit of this device is that it does not contain any information about the user. Thus, if it is lost or stolen, any other person who comes in possession of the device cannot use it to fake access to your services.

Summary of the Invention

The object of the present invention is to provide a portable device as disclosed in WO 2014/021721 with a highly improved personal security level of a user. The invention is a personal identification solution to secure one (1) user, having many safety functions such as flushing the RAM after each identification cyclus, secure each person using a production series number creating each unit unique with the user.

Another invention is to generate a unique biometric identification of a user, as needed by the suppliers, without reviling her/his real biometric images. The invention is based on a solution to generate secure personal cyber biometrical identification, unique to only the user, without compromising his real biometric values, giving the user the same options to change his cyber biometric identification if stolen, same as for cods and password when lost or stolen.

This is achieved in a method, system, device and equipment as defined in the following claims.

In particular, the present invention relates to a method for authenticating a user of a system providing access to a service, the system including any service equipment and a portable device communicating wirelessly with each other, the service equipment including or having access to a storage containing biometric data relating to said user, the portable device including a multitude of biometric readers, wherein the method including the steps of:
the service equipment requesting the portable device to perform at least two different selected biometric readings on the user,

the portable device performing said biometric readings on the user, combining said biometric readings forming a new mixed biometric identity of the user and transmitting the new mixed biometric identity to the service equipment, the service equipment comparing the received mixed biometric identity with the stored biometric data, and if said received and stored biometric data agree, allowing the user access to the service.

The combination of at least two different biometric readings provides extra high security as the invented device mixes two or more biometric readings in order to provide, produce a new biometric image, without revealing the real identity of the original biometric images. The new image, a Cyber biometric image looking like and will be identified as any other biometric identifications used in the digital market for a user.

As the invented device create a unique Cyber biometric image, of the user, using a mix of biometric readings, mechanical selection and a production solution and the new cyber biometric image look like standard biometric images from fingers, Iris, voice and face shape it will function as normal identifications used in Window 10, Android and iOS in mobile, PC, PAD, on internet, on payment terminals and banking without using the real biometric values.

In the signals sent from the portable device to the service equipment, it is very difficult for a potential intruder to deduce which parts of the signals that belongs to which biometric reading and the personal safety for the user is obtain, even if stolen by criminals and hackers.

In a preferred embodiment of the system, all said biometric readings are selected at random by the service equipment, or that one of the biometric readings is selected by the user, the other biometric readings being selected at random by the service equipment, or that all biometric readings are selected at random by the portable device. The benefit of this system is that someone trying to get unauthorized access to the system cannot foresee what information that must be provided in order to get the access.

According to the invention, a production serial number may be stored in the portable device, the portable device being adapted to combine the production serial number, or a part of the production serial number, with the biometric readings before transmitting the result to the service equipment.

The portable device may be adapted to encrypt the communication sent to the service equipment at the personal user selection.

When the portable device is used to identify a access or start up a single smart unit we recommend the personal user to select Bluetooth 4.3 communication, giving an encrypted security level quite impossible to use eavesdropping data as the same image change its encryptions, each time it is transmitted, so hackers can`t match the Cyber biometric image stored in the equipment.

Brief Description of the Drawings

The invention is now to be described in detail in reference to the appended drawings, in which:

Fig. 1a is a schematic illustration in front view of a portable identification device according to the present invention,

Fig. 1b shows the device in side view,

Fig. 1c shows the back side of the inventive portable device,

Fig. 2 is a schematic circuit diagram of the inventive portable device, and

Fig.3 is a schematic diagram of the inventive system with portable device and service equipment.

Detailed Description

As shown in the drawings, the invention relates to a small portable device 1 that is communicating with your personal equipment for starting up and accessing service equipment 20 (fig. 3) providing access to a service 21, 23. When starting up or when approaching service equipment 20 the system will request identification information about the user. The device 1 will then identify the user using multi biometric scanning, and provide clearing information to the equipment providing access to the service. The service in question may be physical actions such as unlocking the front door of your house, opening and starting your car, or procedures such as logging in to any service on the internet, withdrawing cash from cash machines, etc. It will be unnecessary to remember usernames, puck codes, passwords and so on as the inventive device recognizes and can authorize you.

In order to improve the personal security level, the service equipment is adapted to request the portable device 1 to provide several different biometric readings of the user, and provide the readings as a mix as the invented device can mix two or more biometric readings in order to provide a new biometric image or identity, without revealing the real identity of the original biometric images. The new image, a Cyber biometric image look alike any other biometric identifications used in the digital market for a user. The portable device 1 will then perform the selected biometric readings, combine the biometric readings, possible also with a production serial number which is unique for the portable device and possible also with other information, see below, encrypt the combination and send the result to the service equipment 20. The service equipment 20 will decode the signal from the portable device and compare the received biometric reading mix with stored information to control the identity of the user. The Cyber biometric information may be stored locally 25 in the service equipment, or retrieved from a central server 22.

As an example, two fingers may be scanned to obtain 30 coordinate points for each finger. The points for the two fingers may be combined to obtain a new identity for the user with 60 coordinate points, a "cyber finger print" in which it is impossible to know which points that belong to a particular finger. All sorts of biometric readings may be combined in this way, i.e. fingerprint readings, eye iris scans, voice readings, etc., and which may be converted to e.g. 30 coordinate values before being combined 2 by 2 or 3 by 3, etc. Then a new cyber identity is created, which is not real and is difficult to decode by anyone outside the system, if not impossible. Even if the same eye and the same finger is scanned again, the new biometrical identity will become the same, without disclosing the real individual scan values.

To further strengthen the security level, the service equipment 20 may be adapted to request at least two different biometric readings selected at random, or one biometric reading selected at random, the other biometric reading(s) being selected by the user. The system may also be adapted in such a way that all biometric readings are selected by the user or by the portable device 1 at random.

The point is that the information exchanged between the portable device and the service equipment should not be static, but change each time the user is trying to access some service. Someone eavesdropping on the communication between the portable device and service equipment cannot reuse the information to gain access to the service equipment, even if the encryption algorithm is compromised.

The device acts as a multiple information reader and do not contain or store any personal information. That is, when you use any such device nobody may take benefit or misuse a device if you should lose it in case the device is found by a dishonest person. The invention will protect you as a safe person as no one else can start up and match or use your cyber biometric images to match the images in your digital equipment, even when they are stolen.

As shown in Fig. 2, the device 1 includes a microcomputer chipset 14, RAM 15, and ROM 16. The device includes a number of biometric fingerprint readers 6 – 10, one 6 for the thumb on the front of the device 1 and at least one up to four other fingerprint readers 7 – 10 on the back of the device (Fig. 1a and 1b). Each fingerprint reader may have a double function as a switch button and include a LED source, e.g. in a ring around the reader/button that lights up when the finger is correctly positioned on the fingerprint reader or when the button is depressed.

The device may also include an eye scanner as iris/eye color circle or face shape reader (with a daylight camera 3a and/or a night camera 3b), with option to use Retinal Scan. The device may also include a microphone 11 and loudspeaker 12 providing an audio interface as described in detail in co-pending WO 2014/021721. The device may also include a distance indicator ("proximity badge") and a small display 5, as well as a DNA reader in the future. There is also a smart card reader 4 accessible through a slot 13 at the side of the portable device 1 to read your credit, bank, passport and ID-cards. The device may also have a GPS receiver (Global Positioning System) to verify the location of a portable device before connection to prevent interaction to "pirate systems" occupying space in others computers. The device 1 runs on a rechargeable battery 19 and is turned on/off with a button 2 at the front of the device. The device 1 includes at least one wireless transceiver 18 for communicating with the outside world.

The various units 3-19 are communicating with the computer chipset 14 through buses as shown in Fig. 2.

Preferably, the device should not include any accessible storage means for permanent storage, i.e. no outside part may store instructions in the device. The device is only able to read instructions hard programmed in ROM 16 and the RAM 15 will be flushed after each session. Without data storage you cannot be robbed for biometric data or passwords if the device is lost or stolen. The device will only generate biometric mixed and encrypted data so "your private biometry" remains a secret and cannot be used, i.e. misused, by others. As the device has no

recollection when stolen or lost, your private data and passwords are not compromised.

The inventive device is adapted to read at least two biometric scans identifying the user, mix the readings, encrypt the information and transmit the information to service equipment 20, Fig. 3. The service equipment 20 may be adapted to operate services such as local physical devices 21, but may also provide access to services 23 on the Internet (illustrated with the line 24 in Fig. 3), e.g. for file storage, backup services, bank services, etc. When approaching or starting servicing equipment, e.g. pressing the "power on" button on your portable (PC, Mac®, Pad, Iphone®, Android® ..) it will send a signals to the device 1 to identify the device as an original and un-tampered unit, by checking a QR coded cryptic unique production series number with parity check or other "unidentified" coding before requesting the biometric units to start up.

The communication between the device 1 and equipment 20 is encrypted, preferably using type NFC or Bluetooth® solutions. All signals are scrambled by a security chip such as TPCM type for sending only encrypted data. The device may also be restricted to short range communication (some centimeters or even less) to prevent other parties from receiving and decoding the information. When activating the proximity function between your equipment and the device in your pocket you can also stop others from using an ongoing session when disturbed by coworkers or family. With the proximity function activated you can prevent people using your equipment if you have to leave your powered on units behind. The proximity function uses a "proximity badge" as mentioned above.

Your bankcard, ID card or passport may be read by first inserting it into a slot 13 in the inventive device. Then your biometric readings in the card will be verified by comparing with biometric data read by the device. If both results transmitted wireless to the external equipment from the invention device matches, you are identified as the bankcard, ID card or passport owner/user. This may be a handy solution for making identification for access, admission or payments when shopping.

The invented device provides a Personal Safe, Universal, Cyber biometric Unique identification solution for one (1) user only. IT is made ready to work wireless with all existing and available biometrical identification solution as from Google, Microsoft, Apple, Samsung, Huawei etc. The invented device don`t require to be initiated or used through or in accordance with any "authentication server" as it

function by communicate direct as implemented and matching images in standard solutions as in mobiles, PADS, PC, most doors, internet, online payments, governmental and banking solutions.

C l a i m s

1. A method for authenticating a user of a system providing access to a service (21, 23),
the system including any service equipment (20) and a portable device (1) communicating wirelessly with each other,
the service equipment (20) including or having access to a storage (22, 25) containing biometric data relating to said user,
the portable device (1) including a multitude of biometric readers (3a, b, 6-12),
wherein the method including the steps of:
the service equipment (20) requesting the portable device (1) to perform at least two different selected biometric readings on the user,
the portable device (1) performing said biometric readings on the user, combining said biometric readings forming a new mixed biometric identity of the user and transmitting the new mixed biometric identity to the service equipment (20),
the service equipment (20) comparing the received mixed biometric identity with the stored biometric data, and if said received and stored biometric data agree, allowing the user access to the service (21, 23).

2. A method according to claim 1, wherein all said biometric readings are selected at random by the service equipment (20), or that one of the biometric readings is selected by the user, the other biometric readings being selected at random by the service equipment (20), or that all biometric readings are selected at random by the portable device (1).

3. A method according to claim 1, wherein said biometric readings are also combined with a production serial number of the portable device.

4. A method according to any of the previous claims, wherein the portable device is encrypting the mixed biometric identity transmitted to the service equipment.

5. A system for personal safe authenticating a user of a service (21, 23),
the system including any service equipment (20) and a portable device (1) communicating wirelessly with each other,
the service equipment (20) including or having access to a storage (22, 25) containing biometric data relating to said user,
the portable device (1) including a multitude of biometric readers (3a, b, 6-12),
c h a r a c t e r i z e d i n that the service equipment (20) is adapted to

request the portable device (1) to perform at least two different selected biometric readings on the user,
the portable device (1) being adapted to perform said selected biometric readings on the user, combine the biometric readings forming a new mixed biometric identity for the user and transmit the new biometric identity to the service equipment (20), the service equipment (20) being adapted to compare the received bbiometric identity with the stored biometric data, and if said received and stored biometric data agree, to allow the user access to the service (21, 23).

6. The system of claim 5, wherein all said biometric readings are selected at random by the service equipment (20), or that one of the biometric readings is selected by the user, the other biometric readings being selected at random by the service equipment (20), or that all biometric readings are selected at random by the portable device (1).

7. The system of claim 5 or 6, wherein a secret alpha numeric production series number is stored in the portable device (1), the portable device being adapted to combine the production serial number, or a part of the production serial number, with said selected mixed biometric readings before forming the new biometric identity and transmitting the result to the service equipment (20).

8. The system of any of the claims 5-7, wherein the portable device is adapted to encrypt the mixed biometric identity transmitted to the service equipment.

9. A portable device to be used in the system of claim 5-8, wherein the portable device includes a CPU chipset (14), ROM (16), workspace RAM (15), a multitude of biometric readers (3a, b, 6-12), wireless communication means (18) and power supply means (19), the device being operated only by data permanently stored in the ROM (16), the workspace RAM (15) being flushed after each operating cycle,
c h a r a c t e r i z e d i n that the portable device (1) is adapted to perform at least two selected biometric readings of a user, combine the readings and transmit the result of the combination to the service equipment (20).

10. A service equipment (20) to be used in the system of claim 5-8, the service equipment (20) including means for providing access to a service (21, 23), communication means, internal (25) or external (22) storage means storing biometric data relating to a user,
c h a r a c t e r i z e d i n that the service equipment is adapted to store

biometric identities, each identity formed by combining at least two different biometric readings of the user, selecting the biometric readings to be provided by the portable device (1) as a combined biometric identity, and comparing said selected mixed biometric identity received from the portable device with similar biometric data from said storage means, said stored biometric data forming a similar unique biometric identity relating to the same user, and if the readings and stored biometric data agree, to provide access for the user to the service.

11. The service equipment of claim 10, wherein at least one of the selected biometric readings are selected at random.

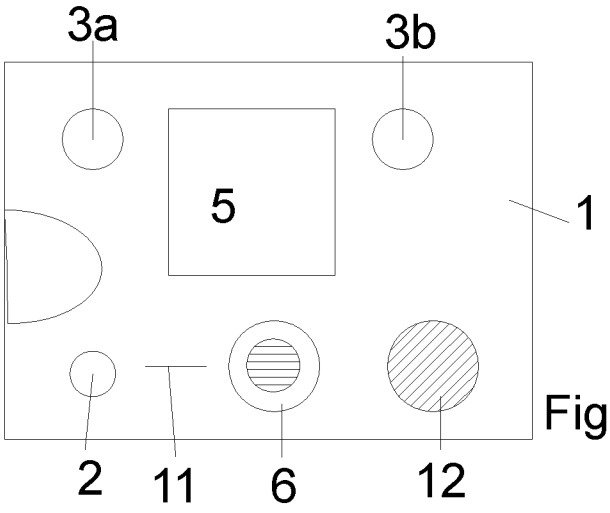

Fig. 1a

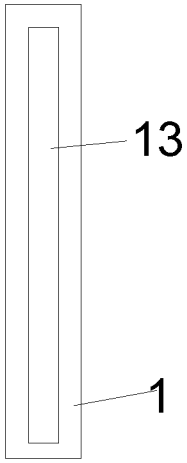

Fig. 1b

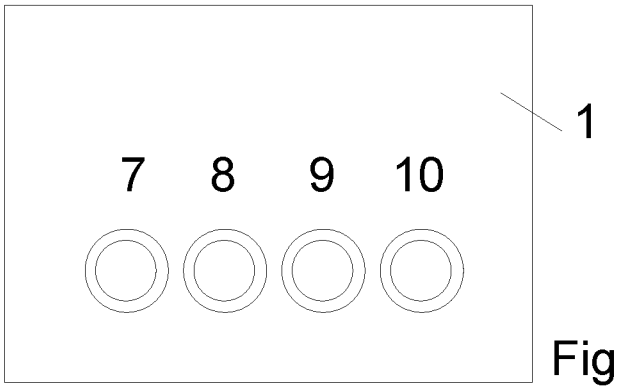

Fig. 1c

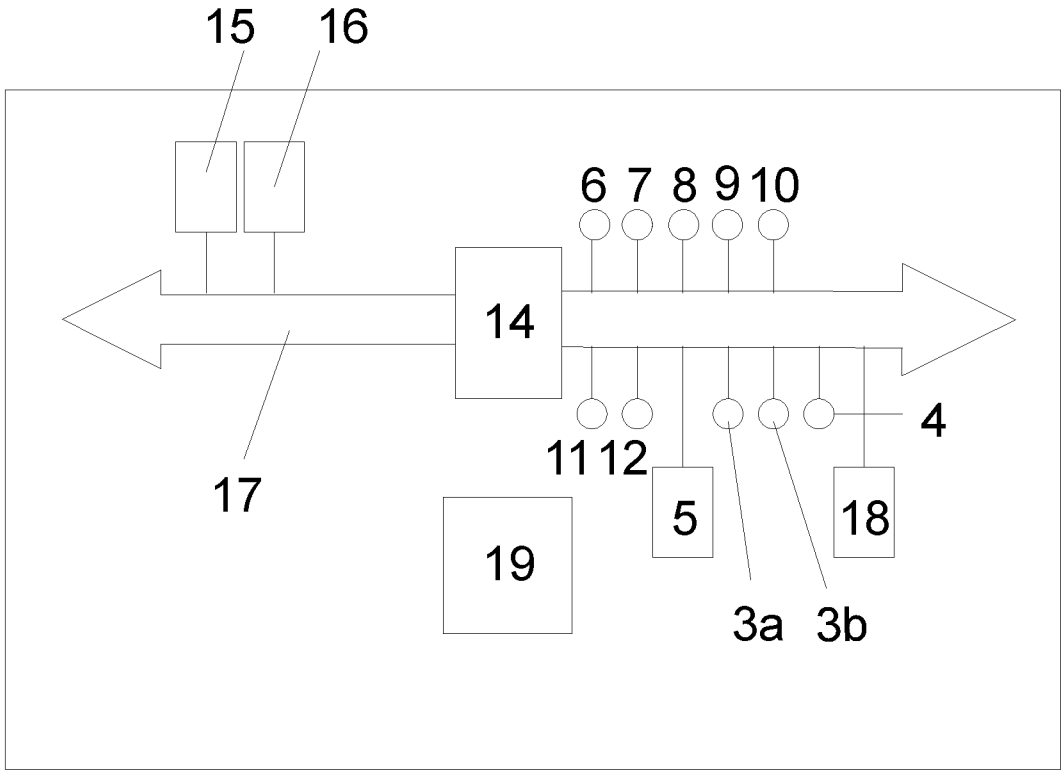

Fig. 2

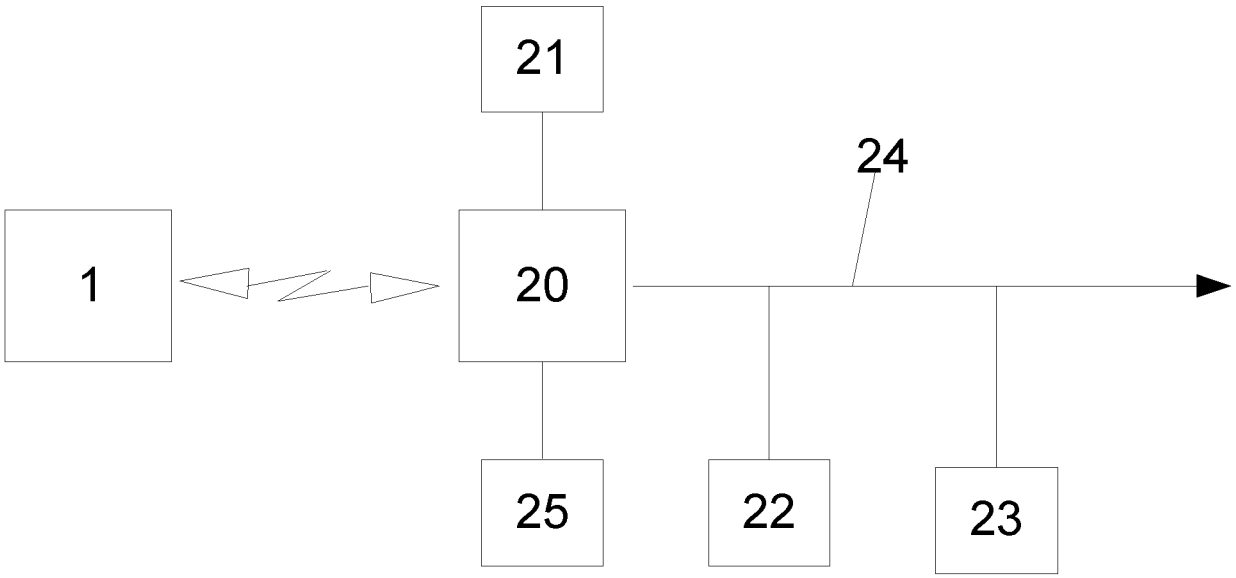

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/NO2017/050011

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32 G06K9/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 696 306 A1 (EKA AS [NO]) 12 February 2014 (2014-02-12) paragraphs [0007], [0009] - [0016] figures 1,2	1-11
A	Christian Rathgeb ET AL: "Multi-Biometric Template Protection: Issues and Challenges" In: "New Trends and Developments in Biometrics", 28 November 2012 (2012-11-28), InTech, XP055363475, ISBN: 978-953-51-0859-7 DOI: 10.5772/52152, paragraphs [02.1], [05.1], [05.5] figure 5	1-11

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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

"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	Date of mailing of the international search report
11 April 2017	20/04/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Segura, Gustavo

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/NO2017/050011

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2013/173926 A1 (MORESE FRANCESCO ANTONIO [US] ET AL) 4 July 2013 (2013-07-04) paragraphs [0078] - [0082] figure 12	1-11
A	WO 2015/109360 A1 (CIRCURRE PTY LTD [AU]) 30 July 2015 (2015-07-30) page 6, lines 1-10 page 9, line 13 - page 13, line 31 figure 5	1-11
A	US 2006/277412 A1 (MANDKE SAMEER [US]) 7 December 2006 (2006-12-07) paragraph [0025]	2,6,11
A	EP 2 151 785 A1 (GEMPLUS [FR]) 10 February 2010 (2010-02-10) paragraphs [0023] - [0040]	1-11

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/NO2017/050011

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2696306 A1	12-02-2014	CN 104508674 A	08-04-2015
		EP 2696306 A1	12-02-2014
		EP 2880586 A1	10-06-2015
		HK 1208928 A1	18-03-2016
		US 2015213659 A1	30-07-2015
		WO 2014021721 A1	06-02-2014
US 2013173926 A1	04-07-2013	NONE	
WO 2015109360 A1	30-07-2015	CN 106415610 A	15-02-2017
		EP 3097515 A1	30-11-2016
		JP 2017508225 A	23-03-2017
		KR 20160111447 A	26-09-2016
		US 2016335426 A1	17-11-2016
		WO 2015109360 A1	30-07-2015
US 2006277412 A1	07-12-2006	NONE	
EP 2151785 A1	10-02-2010	EP 2151785 A1	10-02-2010
		WO 2010012623 A1	04-02-2010