(12) **PATENT**

(11) **344910** (13) **B1**

(19) NO

**NORWAY**

(51) Int Cl.

***G06F 21/32 (2013.01)***
***G06F 21/34 (2013.01)***
*G06F 21/35 (2013.01)*
*G06K 9/62 (2006.01)*
*H04L 29/06 (2006.01)*
*G06K 9/00 (2006.01)*

**Norwegian Industrial Property Office**

| | | | | |
|---|---|---|---|---|
| (21) | Application nr. | 20160057 | (86) | International Filing Date and Application Number |
| (22) | Date of Filing | 2016.01.12 | (85) | Date of Entry into National Phase |
| (24) | Date of Effect | 2016.01.12 | (30) | Priority |
| (41) | Publicly Available | 2017.07.13 | | |
| (45) | Granted | 2020.06.29 | | |

| | | |
|---|---|---|
| (73) | Proprietor | KK88.no AS, Idrettsveien 10, 1400 SKI, Norge |
| (72) | Inventor | Harald Marthinussen, Villaveien 10, 1400 SKI, Norge |
| (74) | Agent or Attorney | OSLO PATENTKONTOR AS, Hoffsveien 1A, 0275 OSLO, Norge |

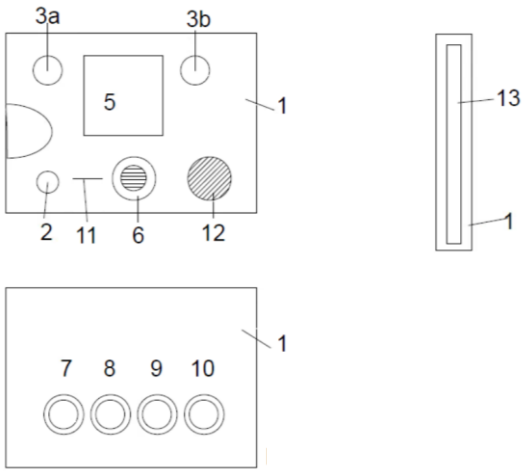
(54) Title **Device for verifying the identity of a person**

(56) References Cited:

US 2015028996 A1, US 2013132091 A1, US 2014289833 A1, US 2005240779 A1, US 2009292641 A1
ROBERTS, C., Biometric attack vectors and defenses, in Computers and Security, Elsevier Science Publishers, pages 14-15, Amsterdam, 2007.02.10.
TAKAHASI, L. et al. Parameter Management Schemes for Cancelable Biometrics, in 2011 IEEE Workshop on Computational Intelligence in Biometrics and Identity Management (CIBIM), pages 145-151, ISSN 2325-4300, IEEE, 2011.
DAVID, et al. A data fusion technique designed for multimodal biometric systems, in Electronics and Telecommunications (ISETC), 2012 10th International Symposium on, pages 155-158, ISBN 978-1-4673-1177-9, IEEE, 2012.
ROSS, et al. Mixing fingerprints for template Security and privacy, in Signal Processing Conference, 2011 19th European, pages 554-558, ISSN 2076-1465, IEEE, 2011
US 2015213659 A1, US 2011191840 A1

(57) Abstract

It is described a system for authenticating a user of a service (21, 23), the system including a service equipment (20) and a portable device (1) communicating wirelessly with each other. The service equipment (20) includes or has access to a storage (22, 25) containing biometric data relating to said user. The portable device (1) includes a multitude of biometric readers (3a, b, 6-12). The service equipment (20) is adapted to request the portable device (1) to perform at least two biometric readings on the user, 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 service equipment (20), the service equipment (20) being adapted to compare the received mixed readings with the stored biometric data, and if said received and stored biometric data agree, to allow the user access to the service (21, 23).



**Field of the Invention**

The present invention relates to a device 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 "Cyberworld" 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.

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.

US 2015028996 discloses methods and systems for biometric authentication solutions with the help of a portable biometric device and an authorized authentication device (AAD)

US 2013132091 discloses a biometric authentication system addressing the vulnerability of raw biometric data and spoofing attacks through a n-dimensional biometric system. Biometric input is randomized through a challenge-response methodology and biometric verification is realized through biometric security tokens unique to the authentication session.

US 2014289833 discloses advanced biometric authentication systems and provisions for authenticating the user's device [0009]. This solution is contrasted against static fusion methods for combining biometric modalities [0017], [0090].

US2005240779 discloses a biometric authentication solution with trusted intermediary biometric(s) reader.

US 2009292641 discloses methods and system for authentication.

Roberts, Chris, Biometric attack vectors and defenses, in Computers and Security, Elsevier Science Publishers, pages 14-25, Amsterdam, 2007.02.10, gives background on well-known challenges and techniques in biometric security solutions.

Takahashi L. et al. Parameter Management Schemes for Cancelable Biometrics, in 2011, IEEE Workshop on Computational Intelligence in Biometrics and Identity Management (CIBIM), pages 145-151, ISSN 2325-4300, IEEE, 2011, describes state of the art of cancellable biometric solutions.

David, et al. A data fusion technique designed for multimodal biometric systems, in Electronics and Telecommunications (ISETC), 2012 10th International Symposium on, pages 155-158, ISBN 978-1-4673-1177-9, IEEE, 2012 and Ross, et al. Mixing fingerprints for template security and privacy, in Signal Processing Conference, 2011 19th European, pages 554-558, ISSN 2076-1465, IEEE, 2011 also describe state of the art of cancellable biometric solutions.

US 20150213659 relates to a device for authenticating a person wherever he goes, the device being handheld, self-contained and handheld with a CPU, RAM, ROM, at least one biometric reader, communication means, a stored unique readable

production series number of the device, and power supply means, the device being operated only by data permanently stored in the ROM, the RAM being flushed after each operating cycle.

US 2011191840 provides an improved biometric authentication methods and systems for providing authenticated user access to or through electronic systems by randomly challenging the user for at least one biometric sample.

**Summary of the Invention**

The object of the present invention is to provide a portable device as disclosed in WO 2014/021721 with an improved security level.

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

In particular, the present invention relates to a system for authenticating a user of a service, the system including a 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. The service equipment is adapted to request the portable device to perform at least two different biometric readings on the user. The portable device is adapted to perform said at least two biometric readings on the user, combining the biometric readings forming a new mixed Cyber identity and transmitting the mixed readings to the service equipment. The service equipment is adapted to compare the received mixed biometric readings with the stored biometric data, and if said received and stored biometric data agree, to allow the user to access the service.

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.

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.

**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 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 banking

automates, etc. It will be unnecessary to remember usernames, puck codes, password and so on as the inventive device recognizes and can authorize you.

In order to improve the 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. 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 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 biological 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 no one else can start up and use 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.

# Claims

1. A method for genetic authenticating of a user of a system providing access to a service (21, 23), without ever putting the user's real biometric values at risk;
the system includes a service equipment (20) and a portable device (1) communicating wirelessly with each other;
the service equipment (20) has access to a storage (22, 25) containing only cyber-biometric-identity (ID) data relating to said user,
the portable device (1) includes a number of biometric readers (3a, b, 6-12) wherein the method includes the steps of:
requesting, via the service equipment (20), the portable device (1) to perform one, two or more different selected biometric readings of the user,
c h a r a c t e r i z e d by the following steps of
   - selecting at random all said biometric readings by the service equipment (20), or
   - selecting one of the biometric readings by the user, and the other biometric readings by the service equipment (20), or
   - selecting at random all biometric readings by the user or the portable device (1),

   - performing, by the portable device (1), said biometric readings of the user,
   - mixing said biometric readings and a secret production serial number of the portable device (1)
   - forming, from the mixed biometric readings and secret production serial number of the portable device (1), a new mixed cyber-biometric-ID of the user, an anonymous type "genetic fake ID" unique to only the user and
   - transmitting the new mixed cyber-biometric-ID, to the service equipment (20),
   - comparing, via the service equipment (20), the received new mixed cyber-biometric-ID with a stored cyber-biometric-ID data and if said received new mixed cyber-biometric-ID and stored cyber-biometric-ID data agree,
   - allowing the user access to the service (21, 23).

2. A method according to claim 1, further comprising encrypting, via the portable device (1), the new mixed cyber-biometric-ID transmitted to the service equipment.

3. A system for personal safe authenticating a user of a service (21, 23), the system includes a service equipment (20) and a portable device (1) communicating wirelessly with each other,

   the service equipment (20) having access to a storage (22, 25) containing a stored cyber-biometric data relating to said user, the portable device (1) including a number of biometric readers (3a, b, 6-2),
   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 of the user, wherein all said biometric readings selected at random by the service equipment (20), or that one of the biometric readings are 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 user or by the portable device (1),

the portable device (1) being adapted to perform said biometric readings of the user, and mixing the biometric readings with a secret production serial number of the portable device (1), forming a new mixed cyber-biometric-ID for the user and transmit the new mixed cyber-biometric-ID to the service equipment (20), the service equipment (20) being adapted to compare the received new mixed cyber-biometric-ID with the stored cyber-biometric-ID data and if said received new mixed cyber-biometric-ID and stored cyber-biometric-ID data agree, to allow the user access to the services (21, 23).

4. A system according to claim 3, wherein the portable device (1) is adapted to encrypt the new mixed cyber-biometric-ID transmitted to the service equipment (20).

5. A portable device (1) to be used in the system of claim 3-4, wherein the portable device (1) includes a CPU chipset (14) ROM (16), workspace RAM (15), a number of biometric readers (3a, b, 6-12), wireless communication means (18) and and power supply means (19), the device (1) being operated only by data permanently stored in the ROM (16) the workspace RAM (15) being flushed after each operating cycle, after each identification
c h a r a c t e r i z e d in that the portable device (1) is adapted to
perform said biometric readings of the user, and mixing the biometric readings with a secret production serial number of the portable device (1), forming a new mixed cyber-biometric-ID for the user and transmit the new mixed cyber-biometric-ID to the service equipment (20).

6. A portable device (1) according to claim 5 wherein the portable device (1) includes separate fingerprint readers (6-10) for each finger on one hand.

7. A service equipment (20) to be used in the system of claim 1, and 3-4, wherein the service equipment (20) includes means for providing access to a service (21, 23) communication means, internal (25) or external (22) storage means storing cyber-biometric-ID data relating to a user,
c h a r a t e r i z e d in that the service equipment is adapted to store cyber-biometric-ID, each identity formed by combining at least two different readings of the user portable device, selecting the cyber-biometric readings to be provided by the portable device (1) to the user as a mixed cyber-biometric-ID, and comparing said selected mixed cyber-biometric-ID received from the portable device (1) with similar cyber-biometric-ID data from said storage means, said stored cyber-biometric-ID forming a similar unique cyber-biometric-ID relating to the same user, and if the received mixed cyber-biometric-ID and stored cyber-biometric-ID data agree, to provide access for the user to the service.

8. A service equipment according to claim 7, wherein at least one of the selected biometric readings are selected at random.

**P a t e n t k r a v**

1. Fremgangsmåte for genetisk autentisering av en bruker av et system som gir tilgang til en tjeneste (21, 23) uten noen gang å sette brukerens virkelige biometriske verdier i fare,
idet systemet omfatter et tjenesteutstyr (20) og en portabel innretning (1) som kommuniserer trådløst med hverandre,
tjenesteutstyret (20) har tilgang til et lager (22, 25) som bare inneholder cyber-biometrisk-identitets (ID) data vedrørende nevnte bruker,
den portable innretningen (1) omfatter et antall biometriske lesere (3a, b, 6-12) hvor fremgangsmåten omfatter trinnene:
forespørsel, via tjenesteutstyret (20), om at den portable innretningen (1) utfører en, to eller flere forskjellige biometriske avlesninger av brukeren,
k a r a k t e r i s e r t v e d de følgende trinn
- tilfeldig utvelgelse av alle nevnte biometriske avlesninger av tjenesteutstyret (20), eller
- utvelgelse av en av de biometriske avlesningene av brukeren, og de andre biometriske avlesningene av tjenesteutstyret (20), eller
- tilfeldig utvelgelse av alle biometriske avlesninger av brukeren eller den portable innretningen (1),
utførelse, av den portable innretningen (1), nevnte biometriske avlesninger av brukeren,
blanding av nevnte biometriske avlesninger med et hemmelig produksjonsserienummer til den portable innretningen (1),
frembringe, fra de blandede biometriske avlesningene og det hemmelige produksjonsserienummeret til den portable innretningen (1), en ny blandet cyber-biometrisk-ID for brukeren, en anonym type «genetisk falsk ID» unik bare for brukeren, og
- sende den nye blandede cyber-biometriske-ID til tjenesteutstyret (20),
- sammenligne, via tjenesteutstyret (20), den nye blandede cyber-biometriske-ID med de lagrede cyber-biometriske-ID data og hvis nevnte mottatte nye blandede cyber-biometriske-ID og de lagrede cyber-biometriske-ID data overensstemmer,
- gi brukeren tilgang til tjenesten (21, 23).

2. Fremgangsmåte ifølge krav 1, videre omfattende kryptering, via den portable innretningen (1), av den nye blandede cyber-biometriske-Iden

sendt til tjenesteutstyret.

3. System for personlig sikker autentisering av en bruker av en tjeneste (21, 23) idet systemet omfatter et tjenesteutstyr (20) og en portabel innretning (1) som kommuniserer trådløst med hverandre,
tjenesteutstyret (20) har tilgang til et lager (22, 25) som inneholder lagrede cyber-biometrisk-identitets (ID) data vedrørende nevnte bruker,
den portable innretningen (1) omfatter et antall biometriske lesere (3a, b, 6-12), k a r a k t e r i s e r t v e d at tjenesteutstyret (20) er innrettet til å forespørre den portable innretningen (1) om å utføre minst to forskjellige biometriske avlesninger av brukeren, hvor alle nevnte biometriske avlesninger utvelges tilfeldig av tjenesteutstyret (20), eller at en av de biometriske avlesningene utvelges av brukeren, og de andre biometriske avlesningene utvelges tilfeldig av tjenesteutstyret (20), eller at alle biometriske avlesninger utvelges tilfeldig av brukeren eller den portable innretningen (1),
den portable innretningen (1) er innrettet til å utføre nevnte biometriske avlesninger av brukeren, og blande de biometriske avlesningene med et hemmelig produksjonsserienummer til den portable innretningen (1), og frembringe en ny blandet cyber-biometrisk-ID for brukeren, og sende den nye blandede cyber-biometriske-ID til tjenesteutstyret (20), idet tjenesteutstyret (20) er innrettet til å sammenligne den nye blandede cyber-biometriske-ID med de lagrede cyber-biometriske-ID data og hvis nevnte mottatte nye blandede cyber-biometriske-ID og de lagrede cyber-biometriske-ID data overensstemmer, å gi brukeren tilgang til tjenesten (21, 23).

4. System ifølge krav 3, hvor den portable innretningen (1) er innrettet til å kryptere den nye blandede cyber-biometriske-ID sendt til tjenesteutstyret (20).

5. Portabel innretning (1) for bruk i systemet ifølge krav 3-4, hvor den portable innretningen (1) omfatter et CPU chipset (14), ROM (16), arbeidsområde-RAM (15), et antall biometriske lesere (3a, b, 6-12), trådløse kommunikasjonsmidler (18) og kraftforsyningsmidler (19), idet innretningen (1) opereres bare av data som er permanent lagret i ROMen (16), og arbeidsområde-RAMen (15) tømmes etter hver operasjonssyklus, etter hver identifikasjon, k a r a k t e r i s e r t v e d at den portable innretningen (1) er innrettet til å utføre nevnte biometriske avlesninger av brukeren og blande de biometriske avlesningene med et hemmelig produksjonsserienummer til den portable innretningen (1), frembringe en ny blandet cyber-biometrisk-ID for brukeren og sende den nye

blandede cyber-biometriske-ID til tjenesteutstyret (20).

6. Portabel innretning (1) ifølge krav 5 hvor den portable innretningen (1) omfatter separate fingeravtrykk-lesere (6-10) for hver finger på en hånd.

7. Tjenesteutstyr (20) for bruk i systemet ifølge krav 1, og 3-4, hvor tjenesteutstyret (20) omfatter midler for å tilveiebringe tilgang til en tjeneste (21, 23), kommunikasjonsmidler, interne (25) eller eksterne (22) lagringsmidler som lagrer cyber-biometriske-ID data vedrørende en bruker, k a r a k t e r i s e r t v e d at tjenesteutstyret er innrettet til å lagre cyber-biometriske-ID, idet hver identitet er frembrakt ved å kombinere minst to forskjellige avlesninger av brukerens portable innretning, utvelge de cyber-biometriske avlesningene som skal tilveiebringes av den portable innretningen (1) til brukeren som en blandet cyber-biometrisk-ID, og sammenligne nevnte utvalgte blandede cyber-biometriske-ID mottatt fra den portable innretningen (1) med tilsvarende cyber-biometriske-ID data fra nevnte lagringsmidler, idet nevnte lagrede cyber-biometriske-ID danner en tilsvarende unik cyber-biometrisk-ID vedrørende den samme brukeren, og hvis den mottatte blandede cyber-biometriske-ID og de lagrede cyber-biometriske-ID data sammenfaller, å gi tilgang for brukeren til tjenesten.

8. Tjenesteutstyr ifølge krav 7, hvor minst en av de utvalgte biometriske avlesningene velges tilfeldig.

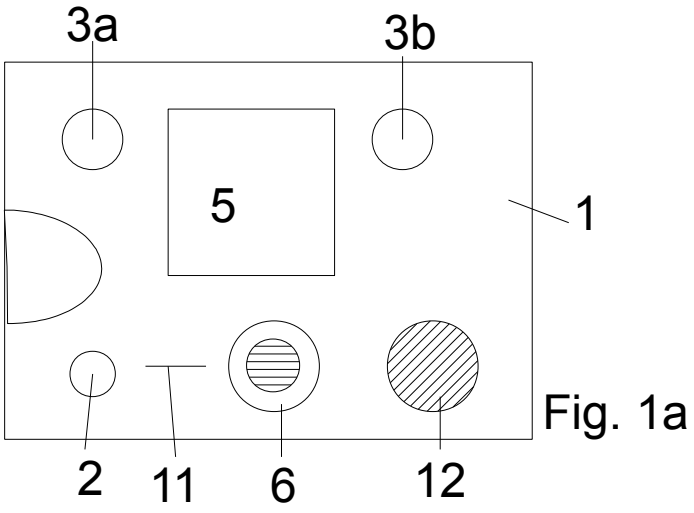



Fig. 1a

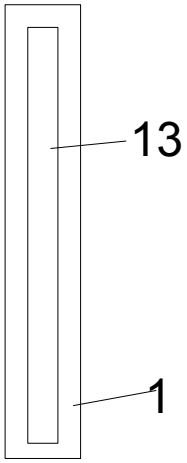



Fig. 1b

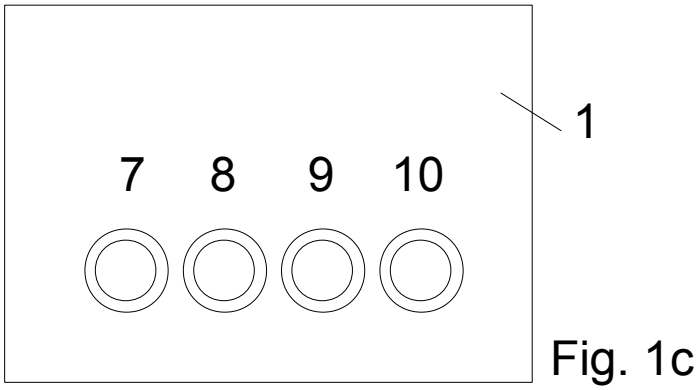



Fig. 1c

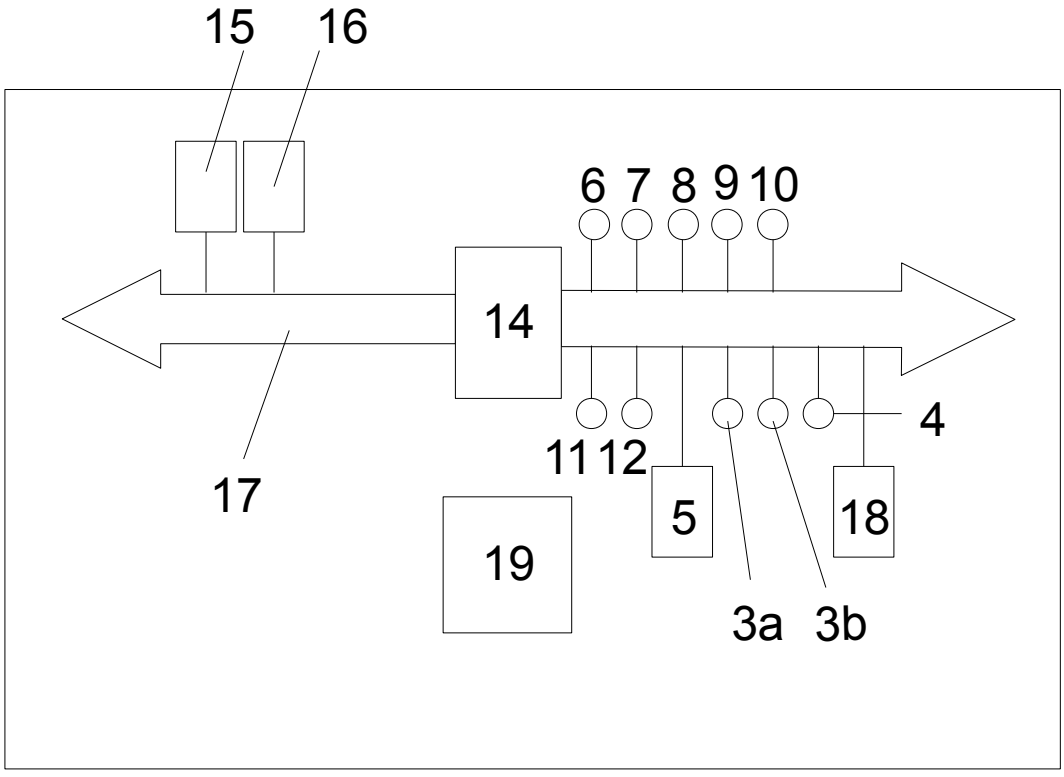



Fig. 2

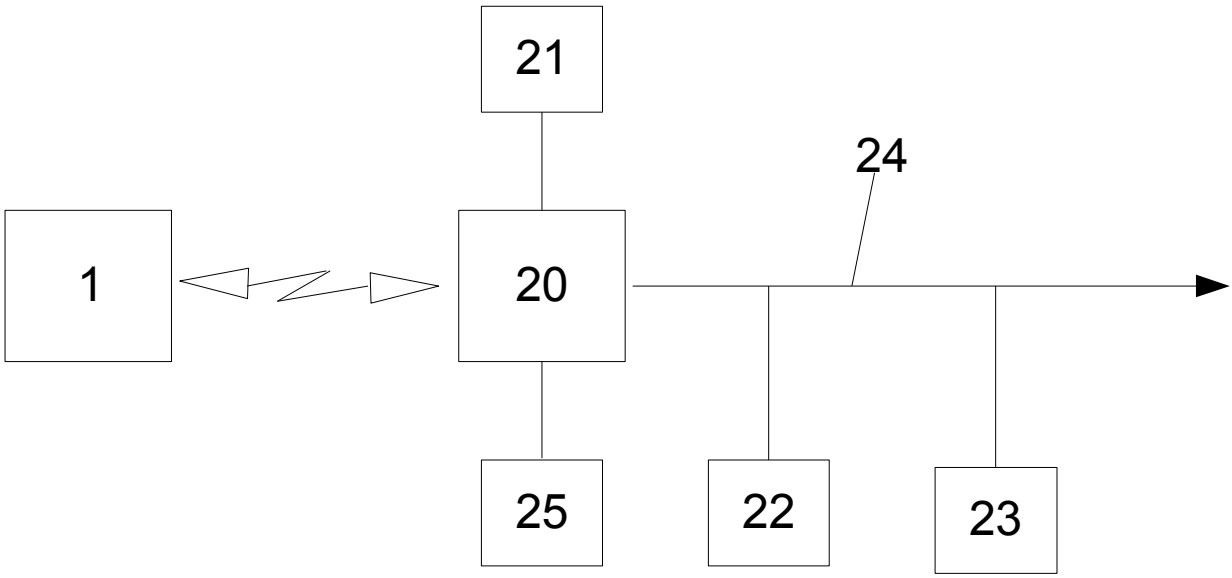



Fig. 3