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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 December 2016 (01.12.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/190829 A1

(51) International Patent Classification:
G06Q 20/40 (2012.01) *G07F 7/10* (2006.01)
G07F 7/08 (2006.01) *G06Q 20/20* (2012.01)

(21) International Application Number:
PCT/TR2016/000076

(22) International Filing Date:
30 May 2016 (30.05.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2015/06503 28 May 2015 (28.05.2015) TR

(71) Applicant: **MT BILGI TEKNOLOJILERI VE DIŞ TIC. A. Ş.** [TR/TR]; Oruçreis DistrictTekstilkent Street Tekstilkent B Blok No:12A/261, Atişalanı, Esenler/İstanbul (TR).

(72) Inventors: **ÇELIK, Aydin**; Tekstilkent Koza Plaza B Blok K.26, Esenler/İstanbul (TR). **SANCAK, Murat**; Tekstilkent Koza Plaza B Blok K.23, Esenler/İstanbul (TR).

(74) Agent: **AKER PATENT-ERKAN AKKAŞ**; Uzunçayır Yolu Street No:51, Kadıköy/İstanbul (TR).

(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, 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, KN, KP, KR, 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).

Published:

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

[Continued on next page]

(54) Title: ID ACCESS DEVICE ENABLING ANY TYPE OF ELECTRONIC PAYMENT FUNCTIONS INCLUDING CONTACT, CONTACTLESS AND BIOMETRIC

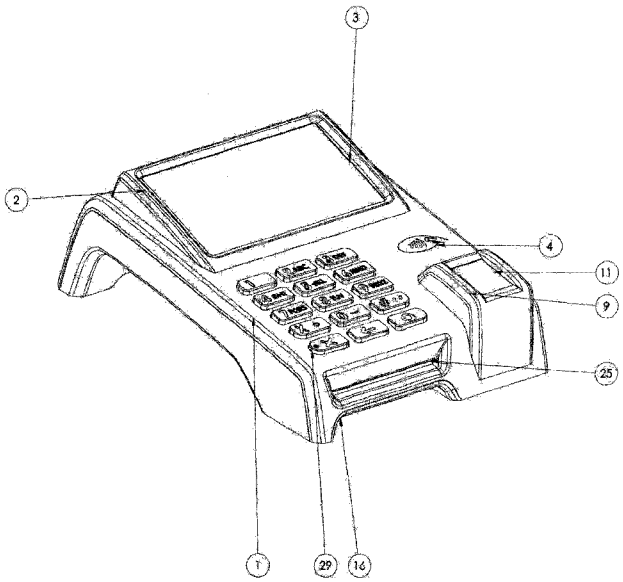

FIGURE 1

(57) Abstract: This invention is about ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric, comprising a top holder (1), screen frame (2), color touch screen (3), contactless reader (4), touch screen capacitive connector (5), touch screen light connector (6), SAM card slot 1 (7), chip card reader zone dedicated to service provider (8), fingerprint and finger vein reader frame (9), USB port for palm vein reader (10), fingerprint and finger vein reader module (11), HDMI connection cable connector (12), external power supply (13), Ethernet interface (14), plastic cover of SAM card slot (15), lower holder (16), USB-Type B(17), mini USB (18). security point 1 on mainboard (19), security point 2 on mainboard (20), 15 connectors of fingerprint and finger vein reader device (21), mainboard lower security cover (22), contactless antenna connector (23), PCB firewall (24), chip card reader zone dedicated to client (25), lock cover of SAM card slot (26), mainboard (27), keyboard illuminated protective area (28), functional password/PIN keys (29), LCD connector (30), button battery (31), micro HDMI (32), battery (33), SIM card slot 1 (34), SEVI card slot 2 (35), recharging module (36) and 20 SAM card slot 2 (37).

WO 2016/190829 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

DESCRIPTION

ID ACCESS DEVICE ENABLING ANY TYPE OF ELECTRONIC PAYMENT FUNCTIONS INCLUDING CONTACT, CONTACTLESS AND BIOMETRIC

This invention is about Contact, Contactless and Biometric ID Access Device Enabling Any Type of Electronic Payment Functions and is an integrated system, which securely aggregates all types of citizens' ID authentication functions in one single electronic card, by which service provider and client are electronically authenticated and contact, contactless and any type of electronic payment transactions can be processed. Our invention comprises a top holder, screen frame, color touchscreen, contactless reader, touchscreen capacitive connector, touchscreen light connector, SAM card slot 1, chip card reader zone dedicated for service provider, fingerprint and finger vein reader frame, USB port for palm vein reader, fingerprint and finger vein reader module, HDMI connection cable connector, external power supply, Ethernet interface, plastic cover of SAM card slot, lower holder, USB-Type B, mini USB, security point 1 on mainboard, security point 2 on mainboard, connectors of fingerprint and finger vein reader device, mainboard lower security cover, contactless antenna connector, PCB firewall, chip card reader zone dedicated for client, lock cover of SAM card slot, mainboard, keyboard illuminated protective zone, functional password/PIN keys, LCD connector, button battery, micro HDMI, battery, SIM card slot 1, SIM card slot 2, recharging module and SAM card slot 2.

STATE OF THE ART

Today, steps for authentication of ID of service provider and client takes places through querying the ID number or ID card of client, which is submitted to authorized person, in the system used by authorized organizations. The step for authentication of service provider in the current system takes place by entering the user card or username and password in the relevant field of electronic authentication devices (i.e. PC) used in the said organization.

In case user card, username and password used in the system of service provider is stolen or becomes available to 3rd parties or ID Card or ID number of client is stolen or becomes available to 3rd parties, then such malicious persons may make transactions resulting in reduced reliability of the authentication measurements.

Due to identity fraud in current system, organizations are subject to loss of goodwill, clients are subject to less secure service acquisition. Insecure transactions may cause both service provider and client to incur material/moral damages as well as substantial economic losses across the country. Increasing rate of cyber-attacks which steal private data aggravates these problems further.

As a result of overall migration to the electronic environments, electronic applications will increasingly be used. The most basic requirement of these applications is to ensure users logging in the systems securely at the service point and a control on them that they act within their authorities assigned to them.

In the state-of-art biometric ID authentication systems, first biometric data of individuals whose IDs will be authenticated are stored in a server, from which in turn retrieved for later ID authentications. Organizations access said servers through cell towers or set up such servers in their organizations. If organizations perform ID authentication through a cell tower, device must be accessible in the coverage of said cell tower. In case of out-of-coverage, then ID authentication cannot be performed. In addition, duration of ID authentication step depends on the number of individuals stored in the ID authentication system. The higher the number of individuals stored there are, then the higher the number of comparisons to be made in order to determine the authentication of ID of an individual is. Therefore, the higher the individuals' data stored there are, the slower the system runs.

Amongst the state-of-art systems of ID authentication system is the ID authentication system via smart card. At the registration stage, biometrically referenced signature of card user is stored in the card memory. There are two options at the ID check stage;

In the first option, a terminal transmits the reference signature predefined in the card from card to terminal in order for ID check and in this case the reference signature open to theft is a disadvantage. In the second option, reference signature is transmitted to card in order to perform a check on the card. Since checking will take very long, system will run slowly.

In the state-of-art system, there is not a solution which will securely perform ID authentication, collection and payment processes in corporate and mobile areas under the same structure.

As a solution to shortcomings of state of art ID authentication systems, our invention is a device which executes ID authentication and transmits the results electronically to ID Authentication Servers in an unfalsifiable manner as well as generates data, valid biometrically and in terms of PIN queries. At this point, our invention is developed in order to meet requirements for integrating ID Cards to be used for personal ID authentication with the ID authentication and payment systems of private use, public/private enterprises providing remote (electronic) service that have all visual and electronic security elements. With secure service provider and client authentication, our invention will avoid frauds committed by the use of ID data of individuals in the service industry, therefore economic losses suffered by the government since it supports state-of-art ID cards with highest level of security. In addition to authentication actions, it performs any kind of contact, contactless, electronic payment transaction in collection and payment systems of the client securely with PIN entry and biometric data verification. In mobile uses of our invention, service is provided to citizens independently of the location. For example, uploading applications of tax office onto our invention will provide a secure environment for citizens to receive services and make payments for such services with their chip ID cards in contact/contactless/electronic methods. Another example is the verification of IDs of drivers who has violated traffic rules enabling onsite collection of payment of fine imposed. Our invention has the infrastructure necessary for making contact/contactless/electronic payment through ID authentication of citizens by providing any kind of actions such as only ID certificate verification, ID certificate and PIN verification, ID certificate and biometric verification, ID certificate and photograph verification, ID certificate, photograph and PIN verification, ID certificate, photograph and biometric verification, ID certificate, photograph, PIN and biometric verification according to security criteria predefined by service providers.

DESCRIPTION OF INVENTION

In our age which world business has been moving to cashless payment as well as ID authentication systems supported with biometric structure has been becoming a part of our lives, combination of these two platforms is an integrated structure which are inseparable from each other that we can describe within innovation criteria. Our invention is a modern payment system, which is designed to facilitate commercial and social services for great masses.

Our invention enables secure storage of next generation ID Cards to be used in place of current generation ID Cards as well as birth details, photograph and biometric data belonging to citizens in the chips of next generation ID Cards and prevents ID cards from being reproduced by unauthorized persons and data inside the ID cards from being modified by such unauthorized persons, namely runs in an integrated manner with the structure which aggregates all ID authentication function in one single electronic card, in which identity data of service provider and client are verified electronically, building an integrated system wherein contact, contactless and any kind of electronic payment is transacted securely. Invention enables verification by means of biometric data, chip ID card and personal verification PINs in the areas such as in-house and mobile uses in hospital, notary public, bank, tax office etc. where security measurements are at advanced levels. Our invention is capable of online and offline verification and in case of any interruption (electric, communication etc.) has the infrastructure which will continue process flow at the same security level.

Our invention has 2 areas of usage such as in-house and mobile use, for in-house uses, it will be used for public and private industry transactions, for mobile uses (police, courier etc.), it will be used for ID authentication by service providers in outdoors as well as for any kind of contact/contactless electronic payment transactions.

Thanks to our invention, ID data of both service provider and client are accessed by Ethernet or mobile communications (GSM, GPRS, 3G, Wi-Fi, Bluetooth etc.) and therefore verification is performed at the highest levels of security as well as in a fast pace depending on the security levels of the card.

Another purpose of our invention is to enable use of different credit cards of different banks in the same one single device. Payment transactions will be performed by supporting NFC technologies of bank applications. System, also, performs 3D secure transactions.

In order to achieve its purpose, invention is built as shown in the annexed Figures ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric;

Figure 1- Front detail view of ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric for Enterprise Use.

Figure 2- Side detail view of ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric for Enterprise Use.

Figure 3- View of the unit located at the back side of the device for more functional use of ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric for Enterprise Use.

Figure 4- Front detail view of ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric for Mobile Uses.

Figure 5- Side detail view of ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric for Mobile Uses.

Figure 6- Bottom detail view of ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric for Mobile Uses.

Figure 7- Assembly detail view of ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric for Enterprise Use.

Parts indicated in the figures are numbered and following is the legend:

1- Top Holder

2- Screen Frame

3- Color Touchscreen

4- Contactless Reader

5- Touchscreen capacitive connector

6- Touchscreen light connector

7- SAM Card Slot 1

8- Chip card reader zone dedicated for service provider

9- Fingerprint and finger vein reader frame

10- USB port of palm vein print reader

11- Fingerprint and finger vein reader module

12- HDMI connection cable connector

13- External power supply

14- Ethernet Interface

15- Plastic Cover of SAM Card Slot

16- Bottom Holder

17- USB-Type B

18- Mini USB

19- Security point 1 on mainboard

20- Security point 2 on mainboard

21- Connector of fingerprint and finger vein reader device

22- Mainboard lower security cover

23- Contactless antenna connector

24- PCB Firewall

25- Chip card reader zone dedicated for client

26- Locking Cover of SAM Card Slot

27- Mainboard

28- Keyboard illuminated protective zone

29- Functional password/PIN keys

30- LCD connector

31- Button battery

32- Micro HDMI

33- Battery

34- SIM Card Slot 1

35- SIM Card Slot 2

36- Recharging module

37- SAM Card Slot 2

DETAILED DESCRIPTION OF INVENTION

This structure has one chip card reader (25), by which client verify his ID card data, on the front side and a second chip card reader (8), by which service provider verify his ID card data, on the back side as well as fingerprint and finger vein reader module (11), by which servicer provider and client have their fingerprints read. Other biometric readers (finger vein, palm, retina etc.), other than fingerprint reader, can be connected externally to the device. There is a color touchscreen (3), which will display summary data of chip card read or biometric data that are received by communicating with authorized organization (ID Authentication Unit) as well as photographs and by which signature will be received.

After data matching, device deletes such data automatically. In order to make operation of device more functional, device has a separate unit that comprises an Ethernet interface (14), mini USB (18), USB Type-B (17) and power supply (13). Its separate design is in order to make actions for service provider and client.

In addition to verification of ID data by service provider and client, device will enable any kind of contact, contactless and any kind of payment transactions, thanks to its EFT-POS functionality by connecting to New Generation payment recording devices. The device has a functional keypad (29) for entering password/PIN of chip cards of users during verification as well as contactless reader zone (4) located on the front side of the device for contactless transactions. Thus, transaction payments, such as bank, notary, will be made at that time with contact/contactless payment options thanks to EFT-POS functionality. The device has a battery (33) which ensures continuity of verification and collection operations by supplying power to our device during electricity outage in the cases of mobile uses, and a recharging connector zone (36) which recharges the battery ensuring the continuity of operations. There are two units of SIM card slots (34, 35) for mobile uses, and micro HDMI zone (32) for data transfer, recharging battery and Ethernet connection.

Our invention is equipped with secure software and hardware architecture meeting the common criteria for possible external attacks. Since our invention performs data transfer via EAL 4+ secure software and with authorized organizations, it is designed with a structure which allows only intervention by authorized personnel in the cases of possible failures. The device has the advanced level of security architecture, which will meet PCI-PTS, international security standards in payment transactions, has EMV L1/L2 for contact transactions as well as enable secure operations with VISA, MASTERCARD, AMEX and JCB cards which will support authorized contactless software. This structure is provided with tampering sensor mechanisms on the mainboard.

For turning on the device, the power supply (13) is plugged to wall outlets and for accessing secure local network connection and organizational applications, Ethernet (LAN) cable is plugged to Ethernet interface (14). For mobile uses, for GSM, GPRS, 3G etc. communication types, SIM cards are inserted to SIM card slots (34, 35).

In mobile uses, there is a micro HDMI zone (32) which is also used as Ethernet connection, data transfer and battery power supply. Our device becomes functional after having made the power cables and Internet connections. When process flow is initiated between service provider and client, the client inserts his ID card in the chip card reader dedicated for client (25) located on the front side of the device, the service provider inserts his card in the chip card reader dedicated for service provider (8) located on the back side of the device. Then, on the basis of security criteria predefined by service providers, a couple more data entry via devices externally connected to our device (fingerprint, palm, retina readers etc.) can be made. (Only ID authentication, ID authentication and PIN, ID authentication and biometric verification, ID and photograph verification, ID, photograph and PIN verification, ID, photograph and biometric verification etc.)

Summary data received after communicating these data with ID Authentication Unit will be displayed on the color touchscreen (3). After verification, if any, any collections will be made via contact/contactless any kind of electronic payment options instantly. For contactless payment, contactless card reader (4) is used and for contact payments, chip card reader zone dedicated for client (25), and functional keypad for PIN/password entry (29) are used. In the transactions requiring signature, signatures can be affixed on color touchscreen (3). Thanks to our device, payment transactions in public and private organizations will be recorded in the governmental registries. Therefore, no illicit transactions will be made, goodwill and material losses due to identity fraud in the current system will be precluded and citizens will be ensured to receive secure and fast service via one single card.

This invention is about ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric comprising a top holder (1), screen frame (2), color touchscreen (3), contactless reader (4), touchscreen capacitive connector (5), touchscreen light connector (6), SAM card slot 1 (7), chip card reader zone dedicated for service provider (8), fingerprint and finger vein reader frame (9), USB port for palm vein reader (10), fingerprint and finger vein reader module (11), HDMI connection cable connector (12), external power supply (13), Ethernet interface (14), plastic cover of SAM card slot (15), lower holder (16), USB-Type B(17), mini USB (18), security point 1 on mainboard (19), security point 2 on mainboard (20), connector of fingerprint and finger vein reader device (21), mainboard lower security cover (22), contactless antenna connector (23), PCB firewall (24), chip card reader zone dedicated for client (25), lock

cover of SAM card slot (26), mainboard (27), keyboard illuminated protective zone (28), functional password/PIN keys (29), LCD connector (30), button battery (31), micro HDMI (32), battery (33), SIM card slot 1 (34), SIM card slot 2 (35), recharging module (36) and SAM card slot 2 (37).

CLAIMS

1- This invention is about ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric comprising a top holder (1), screen frame (2), color touchscreen (3), contactless reader (4), touchscreen capacitive connector (5), touchscreen light connector (6), SAM card slot 1 (7), chip card reader zone dedicated for service provider (8), fingerprint and finger vein reader frame (9), USB port for palm 10 vein reader (10), fingerprint and finger vein reader module (11), HDMI connection cable connector (12), external power supply (13), Ethernet interface (14), plastic cover of SAM card slot (15), lower holder (16), USB-Type B(17), mini USB (18), security point 1 on mainboard (19), security point 2 on mainboard (20), 15 connectors of fingerprint and finger vein reader device (21), mainboard lower security cover (22), contactless antenna connector (23), PCB firewall (24), chip card reader zone dedicated for client (25), lock cover of SAM card slot (26), mainboard (27), keyboard illuminated protective zone (28), functional password/PIN keys (29), LCD connector (30), button battery (31), micro HDMI (32), battery (33), SIM card slot 1 (34), SIM card slot 2 (35), recharging module (36) and 20 SAM card slot 2 (37).

2- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said top holder comprises color touchscreen (3), functional password/PIN keys (29), chip card readers (8, 25) and fingerprint and finger vein reader module (11).

3- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said color touchscreen (3), where data are displayed, comprises a protective screen frame (2) which protects it against scratches and impacts.

4- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a color touchscreen (3) in which data of service provider and client are displayed, which is capable of obtaining signature for authentication and service agreements.

5- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a contactless reader (4) which is capable of processing contactless payment transactions.

6- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a color touchscreen capacitive connector (5) for making actions by touching on color touchscreen (3) as well as obtaining on the screen the personal signature data of both service provider and client.

7- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a touchscreen light connector (6) required for illuminated panel of touchscreen (3).

8- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein a lower holder (16) comprises a SAM Card Slot 1 (7) for the use of EFT-POS users.

9- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a chip card reader zone dedicated to service provider (8) through which service provider have his chip ID card read.

10- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a biometric fingerprint and finger vein reader frame (9) which protects fingerprint and finger vein reader module (11).

11- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a USB port of palm vein print reader (10) which can be connected to use the palm reader device in compliant with our invention.

12- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a biometric fingerprint and finger vein reader module (11) through which finger vein print and any kind of biometric verification data of service provider and client are read.

13- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a HDMI connection cable connector (12) required for connection of HDMI cable from external peripheral connection providers.

14- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein an external apparatus comprises an external power supply (13) to which a power supply can be connected.

15- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein an external apparatus comprises an Ethernet interface (14).

16- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein the SAM Card slot comprises a plastic cover (15) in order to protect SAM card, once inserted in said slot, against external factors.

17- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein a lower holder (16) comprises the parts of top holder and the internal connection units.

18- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein the external apparatus comprises a USB-Type B (17).

19- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein the external apparatus comprises a Mini USB (18).

20- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein the protective mainboard comprises the security point 1 (19) which acts as one of main security points of mainboard and will protect device against unauthorized tampering and if subjected to tampering, then prevent interventions other than authorized personnel.

21- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein the protective mainboard comprises the security point 2 (20) which acts as one of main security points of mainboard and will protect device against unauthorized tampering and if subjected to tampering, then prevent interventions other than authorized personnel.

22- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein fingerprint and finger vein reader device comprises a connection connector (21) which is required for fingerprint and finger vein reader module (11) to operate in consistent with our invention.

23- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises the mainboard lower security cover (22) which will ensure protection of operating and security system of our invention.

24- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a contactless antenna connector (23) which is capable of processing contactless transactions in our invention.

25- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a protective PCB firewall (24) in order to protect security system of our invention.

26- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a chip card reader zone dedicated to client (25) through which client have his chip ID card/credit card read.

27- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein the SAM Card slot comprises a locking cover (26) in order to protect SAM card slot against external impacts.

28- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a mainboard (27) which comprises operating and security system.

29- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprise a keyboard-illuminated protective zone (28) which enables keyboard containing keypad (29) to be illuminated.

30- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises functional password/PIN keys (29) through which password/PIN of ID card and bank/credit card are keyed in.

31- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a LCD connector (30) which enables operation of capacitive screen of our invention.

32- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprise a button battery (31), inserted in battery unit on the main board, which enables security processor to run even if device shutdown.

33- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises micro HDMI (32) to be used for recharging mobile device with connection cable, enabling data transfer and Ethernet connections.

34- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a battery (33) which acts as a power supply for mobile uses.

35- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a SIM card slot 1 (34) to which SIM Card can be inserted for mobile uses.

36- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a SIM card slot 2 (35) to which SIM Card can be inserted for mobile uses.

37- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a recharging module (36) which enables device to be charged for mobile uses.

38- The ID Access Device Enabling Any Type of Electronic Payment Functions Including Contact, Contactless and Biometric of Claim 1, wherein said device comprises a SAM card slot 2 (37), located in a hidden place of mainboard (27), which is for the use of GEM Card, which will be obtained from authorized organizations.

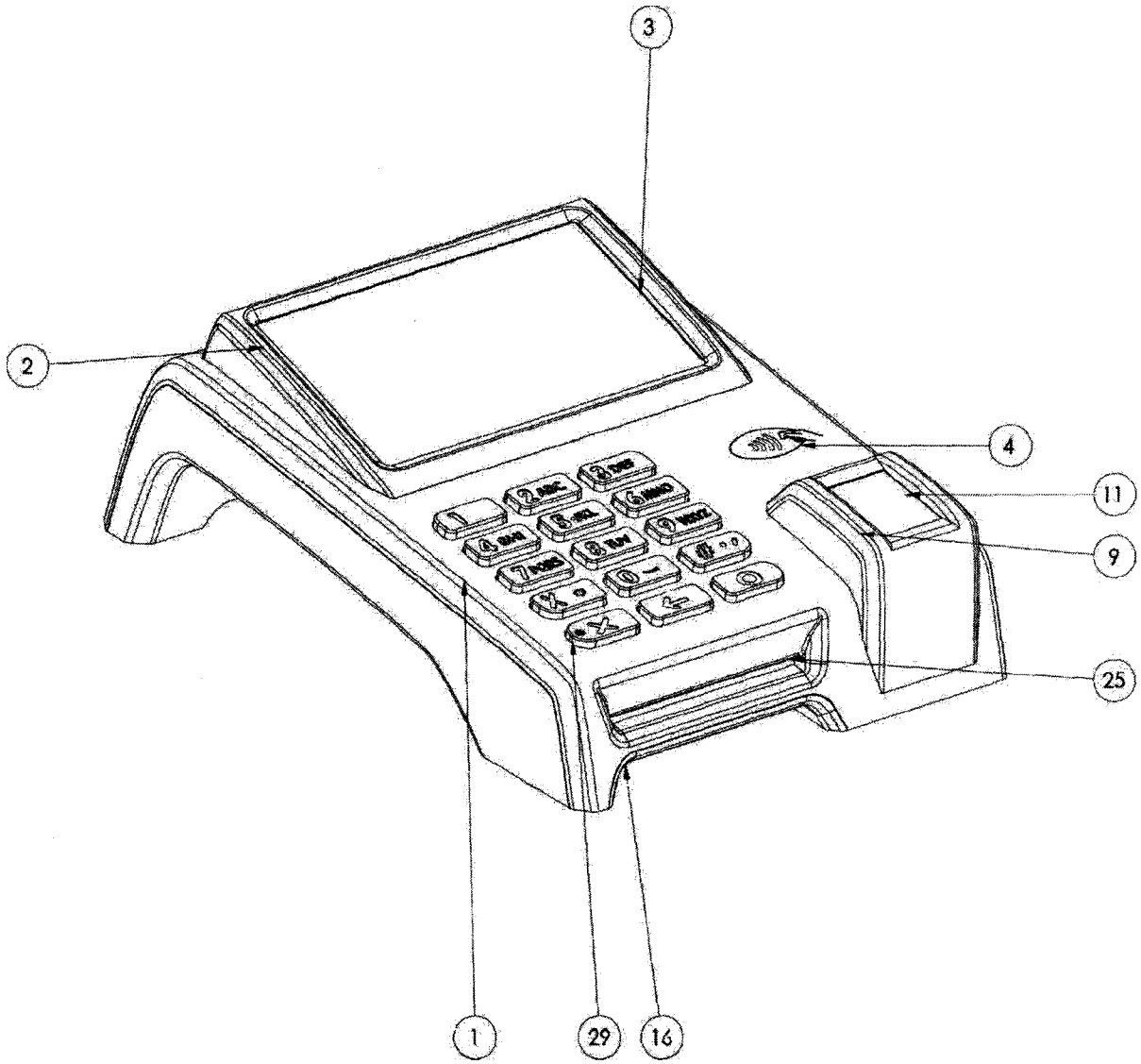

FIGURE 1

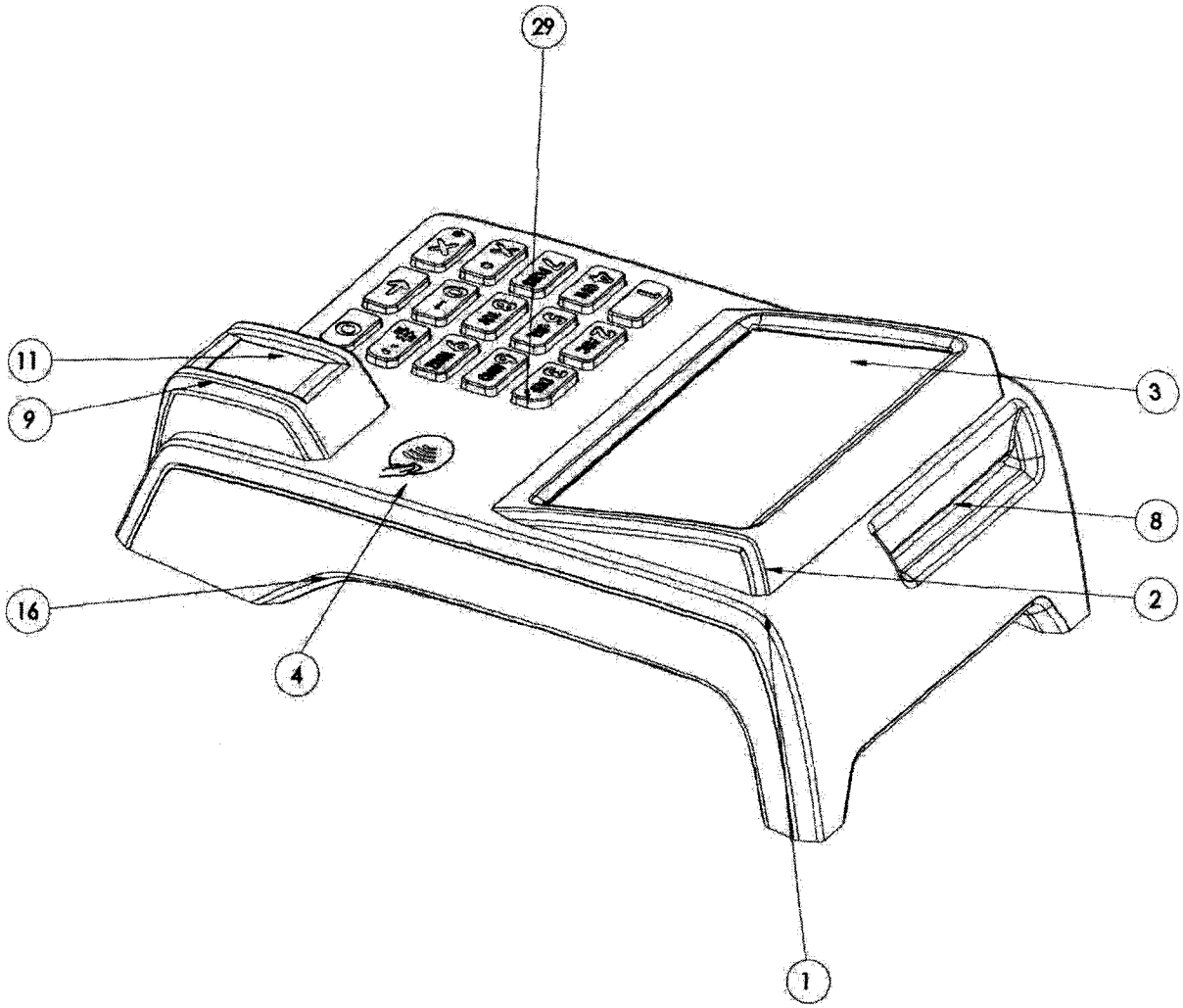

FIGURE 2

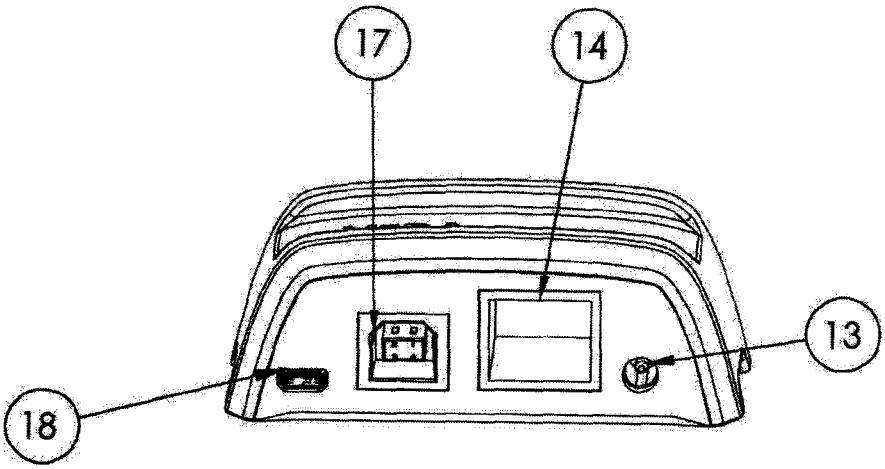

FIGURE 3

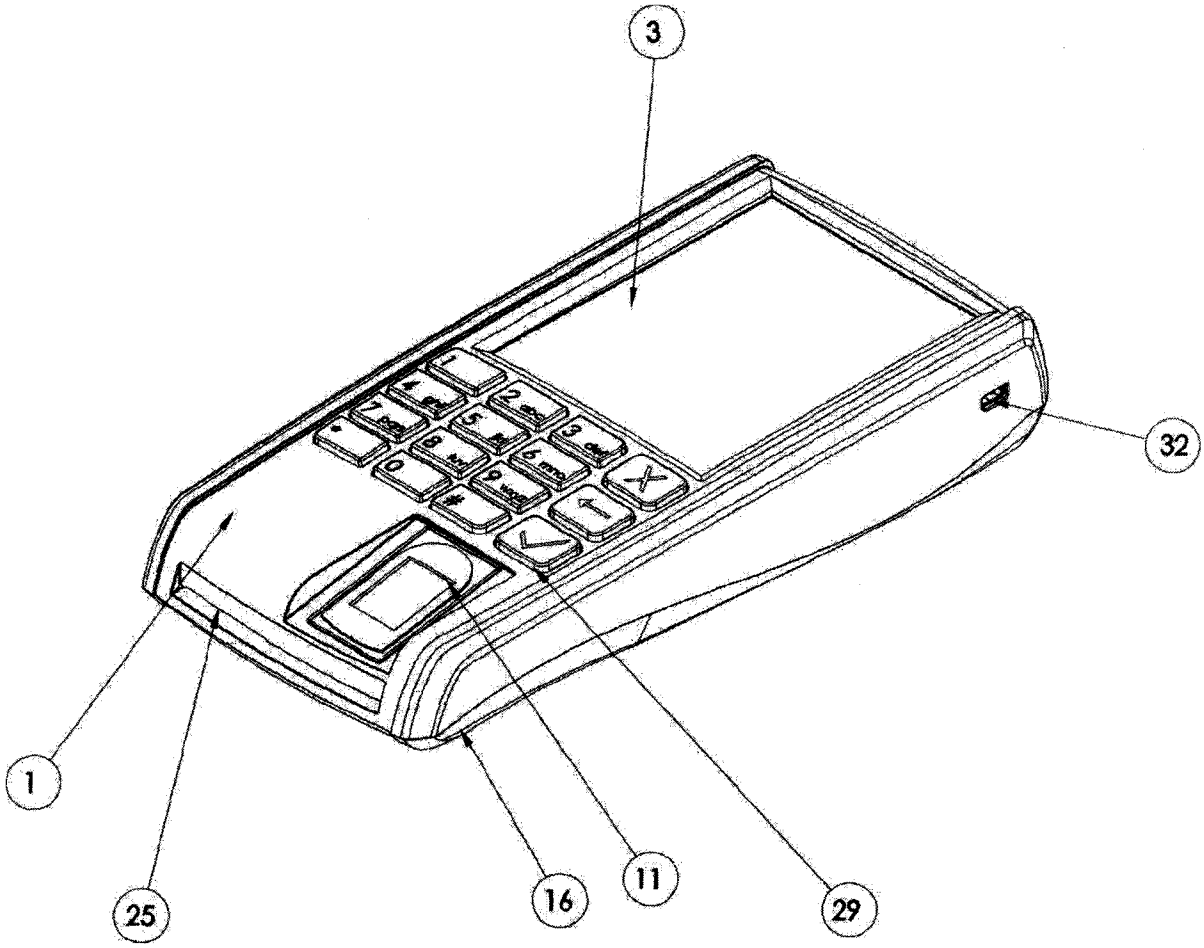

FIGURE 4

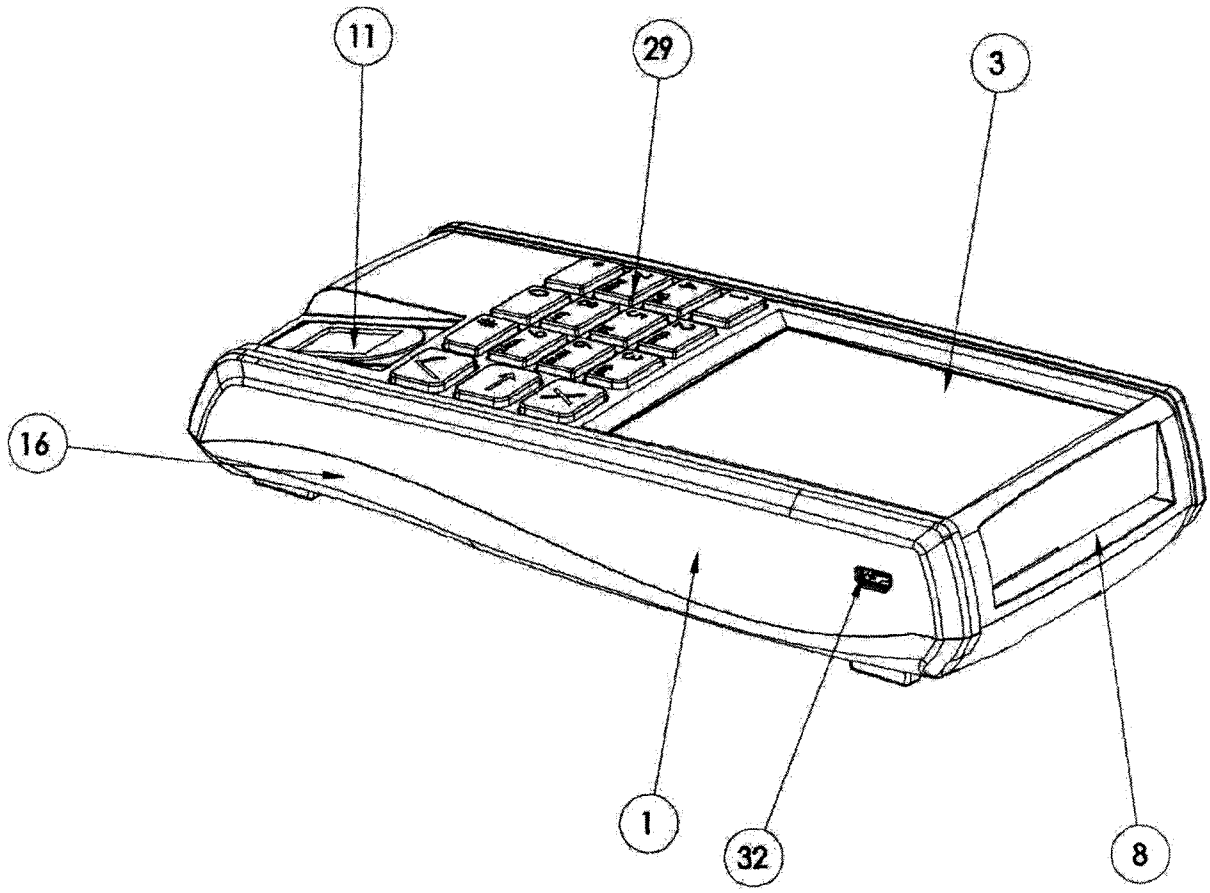

FIGURE 5

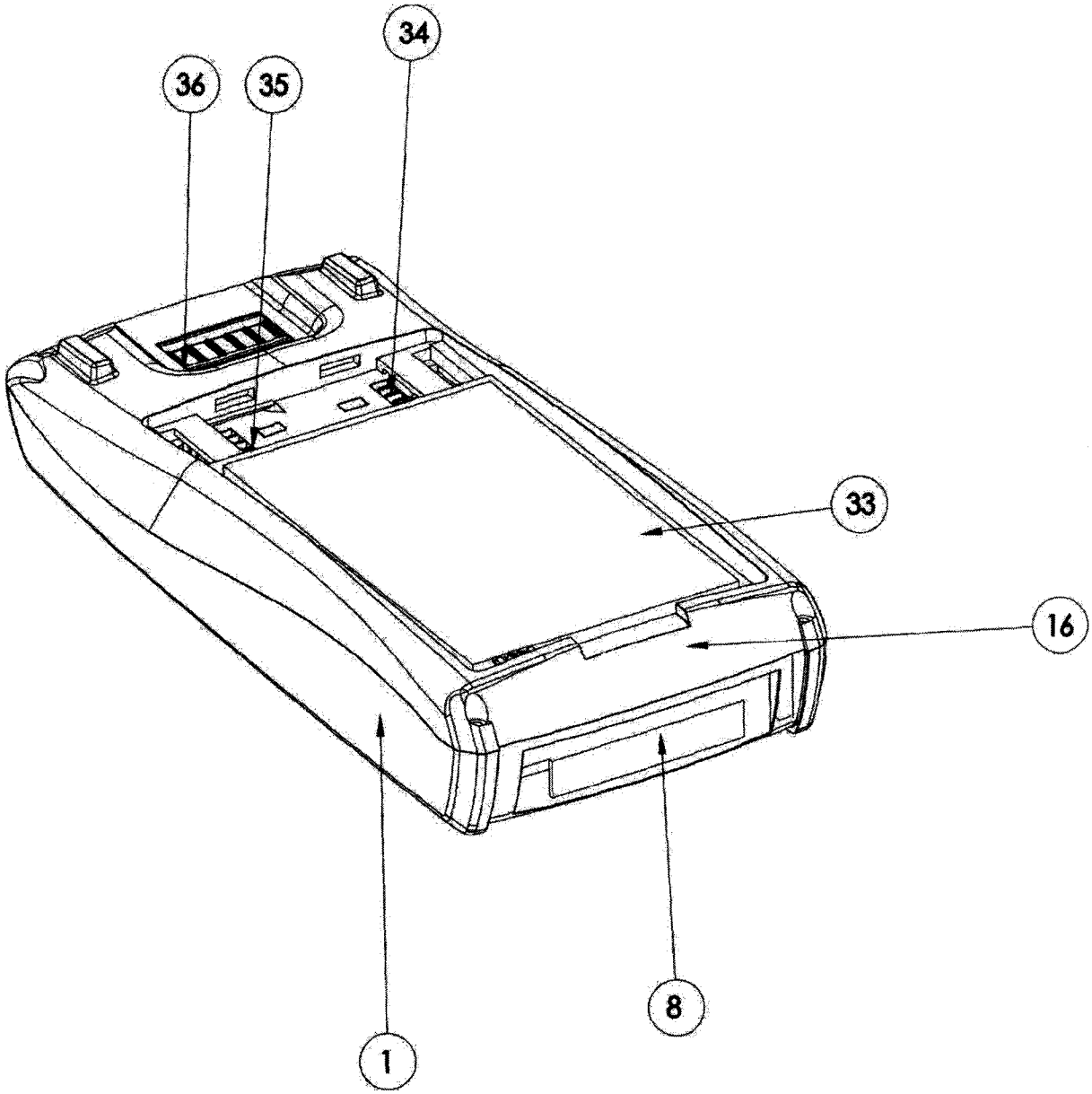

FIGURE 6

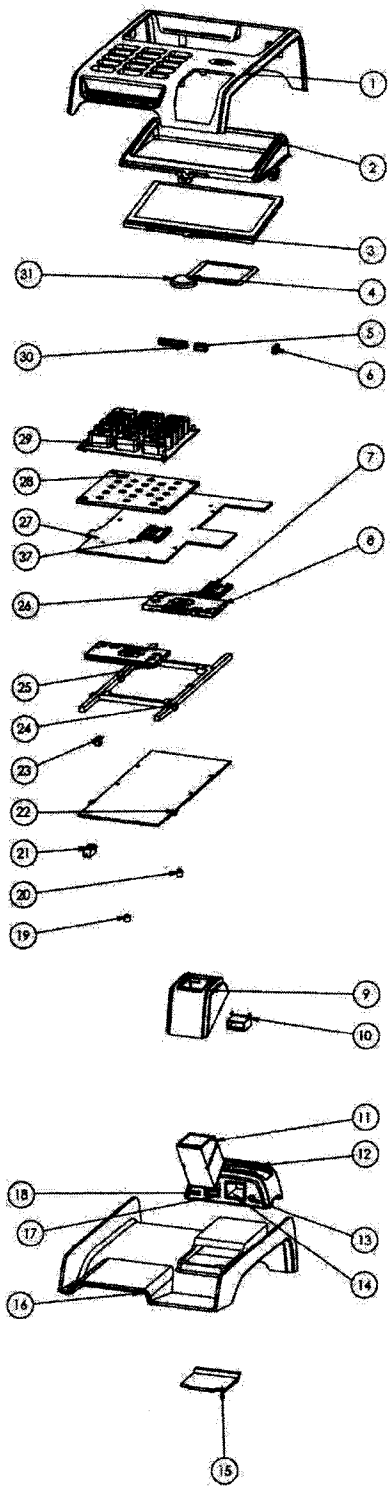
1
2
3
31
4
5
30
6
29
7
28
27
8
37
26
25
24
23
22
21
20
19
9
10
11
12
18
13
17
14
16
15

FIGURE 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/TR2016/000076

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/40 G07F7/08 G07F7/10 G06Q20/20
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)
G06Q G07F

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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/219776 A1 (FINN DAVID [IE]) 5 October 2006 (2006-10-05) abstract; figures paragraphs [0287] - [0312], [0351] - [0381], [0476], [0501] - [0508]	1-38
A	US 2014/183260 A1 (SANCAK MURAT [TR]) 3 July 2014 (2014-07-03) abstract; figures	1-38

-/--

[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
27 October 2016	07/11/2016

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	Breugelmans, Jan

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/TR2016/000076

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	YILDIZ M ET AL: "Combining Biometric ID Cards and Online Credit Card Transactions", DIGITAL SOCIETY, 2010. ICDS '10. FOURTH INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 10 February 2010 (2010-02-10), pages 20-24, XP031649404, ISBN: 978-1-4244-5805-9 the whole document	1-38
X	MÜCAHIT MUTLUGÜN ET AL: "Turkish national electronic identity card", SECURITY OF INFORMATION AND NETWORKS, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA, 6 October 2009 (2009-10-06), pages 14-18, XP058243314, DOI: 10.1145/1626195.1626201 ISBN: 978-1-60558-412-6 the whole document	1-38
A	EP 1 146 487 A2 (BIOCENTRIC SOLUTIONS INC [US]) 17 October 2001 (2001-10-17) figures	1-38
A	WO 2006/010019 A2 (DIGIMARC CORP [US]) 26 January 2006 (2006-01-26) abstract; figures	1-38
A	WO 01/86599 A2 (SUPERCOM LTD [IL]; LANDMAN AVI [IL]; ROZEN ELI [IL]; HASSAN JACOB [IL]) 15 November 2001 (2001-11-15) abstract; figures	1-38
A	US 2008/126260 A1 (COX MARK A [US] ET AL) 29 May 2008 (2008-05-29) abstract; figures	1-38

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/TR2016/000076

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006219776 A1	05-10-2006	NONE	
US 2014183260 A1	03-07-2014	CN 103503039 A	08-01-2014
		US 2014183260 A1	03-07-2014
		WO 2013021233 A1	14-02-2013
EP 1146487 A2	17-10-2001	EP 1146487 A2	17-10-2001
		US 2002030581 A1	14-03-2002
		ZA 200103067 B	02-01-2002
WO 2006010019 A2	26-01-2006	US 2006157559 A1	20-07-2006
		WO 2006010019 A2	26-01-2006
WO 0186599 A2	15-11-2001	AU 5501001 A	20-11-2001
		WO 0186599 A2	15-11-2001
US 2008126260 A1	29-05-2008	NONE	