US 20100203870A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2010/0203870 A1

(43) Pub. Date: Aug. 12, 2010

Hubinak et al.

(54) SYSTEMS AND METHODS FOR CONTACTLESS PAYMENT AUTHORIZATION

(75) Inventors: **Emil Hubinak**, Piestany (SK); **Miroslav Florek**, Bratislava (SK); **Michal Masaryk**, Bratislava (SK)

Correspondence Address:
WOODCOCK WASHBURN LLP
CIRA CENTRE, 12TH FLOOR, 2929 ARCH STREET
PHILADELPHIA, PA 19104-2891 (US)

(73) Assignee: **LOGOMOTION, s.R.O.**, Piestany (SK)

(21) Appl. No.: **12/669,116**

(22) PCT Filed: **Dec. 30, 2008**

(86) PCT No.: **PCT/IB2008/055587**

§ 371 (c)(1),
(2), (4) Date: **Jan. 14, 2010**

(30) **Foreign Application Priority Data**

Jan. 4, 2008 (SK) ..... PP 5004-2008

Publication Classification

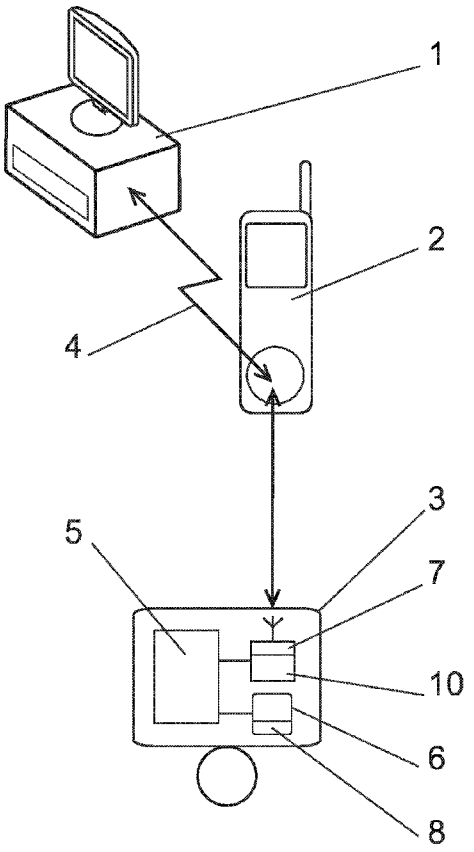
(51) **Int. Cl.**

H04M 3/42	(2006.01)
G06Q 20/00	(2006.01)
H04L 9/32	(2006.01)

(52) **U.S. Cl.** **455/414.1**; 705/44; 705/71; 713/176

(57) **ABSTRACT**

The method and system of authentication of authorized person and transaction approval principally at the direct debits by means of a mobile communication device (**2**) is based on the fact that an alphanumerical chain is sent from the mobile communication device (**2**) into energy passive identifier (**3**) approached to the mobile communication device (**2**), the identifier (**3**) is supplied contact free by electromagnetic field of the mobile communication device (**2**) while in the identifier the received alphanumerical chain is signed electronically and in such signed alphanumerical chain is sent back into the mobile communication device (**2**). Payment approval is realized by the correctness approval of the electronically signed alphanumerical chain and by approaching the mobile communication device (**2**) to the payment terminal (**1**). The invention enables to use a high level of cryptography security by using a passive identifier (**3**) which does not demand own energy source.



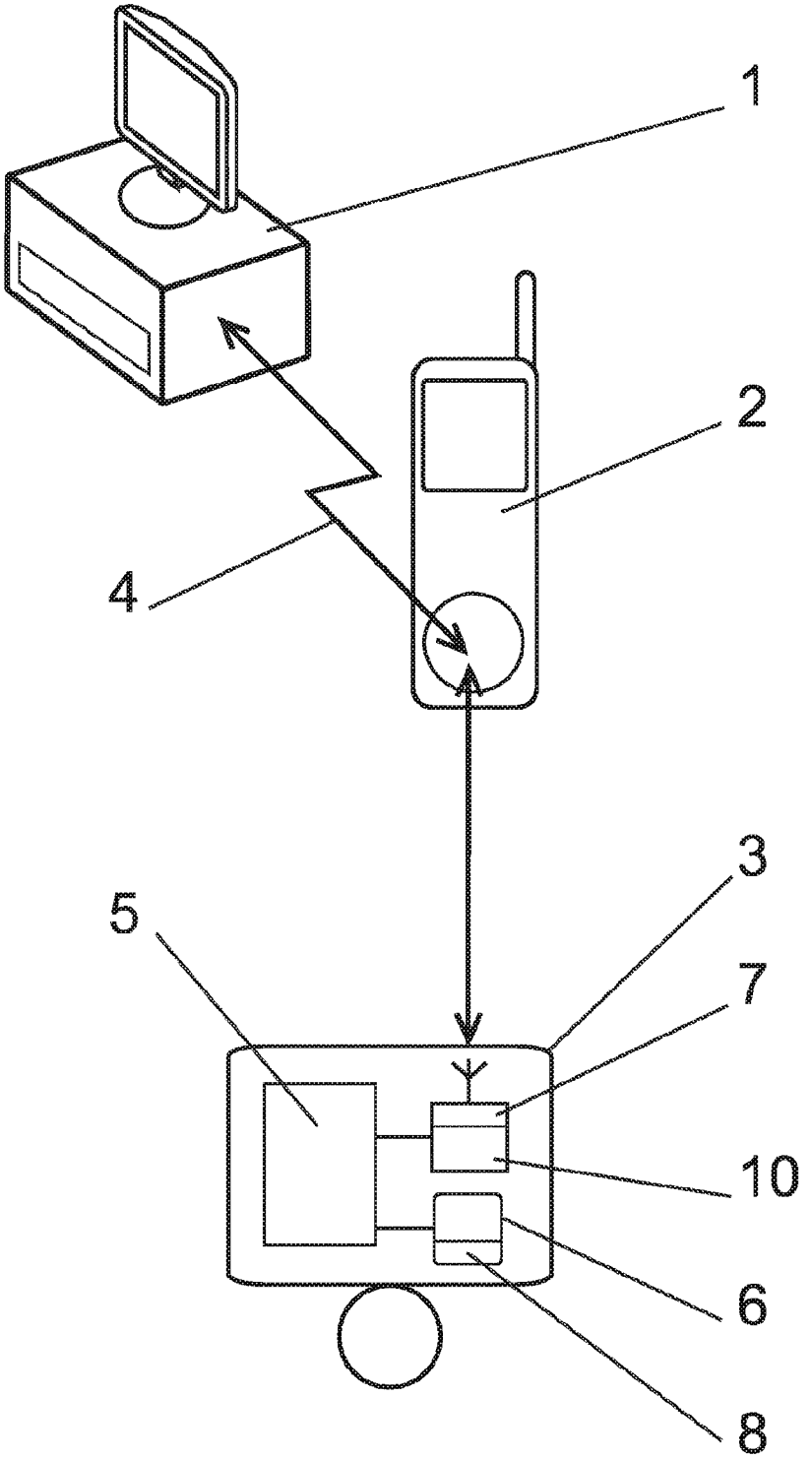


Fig. 1

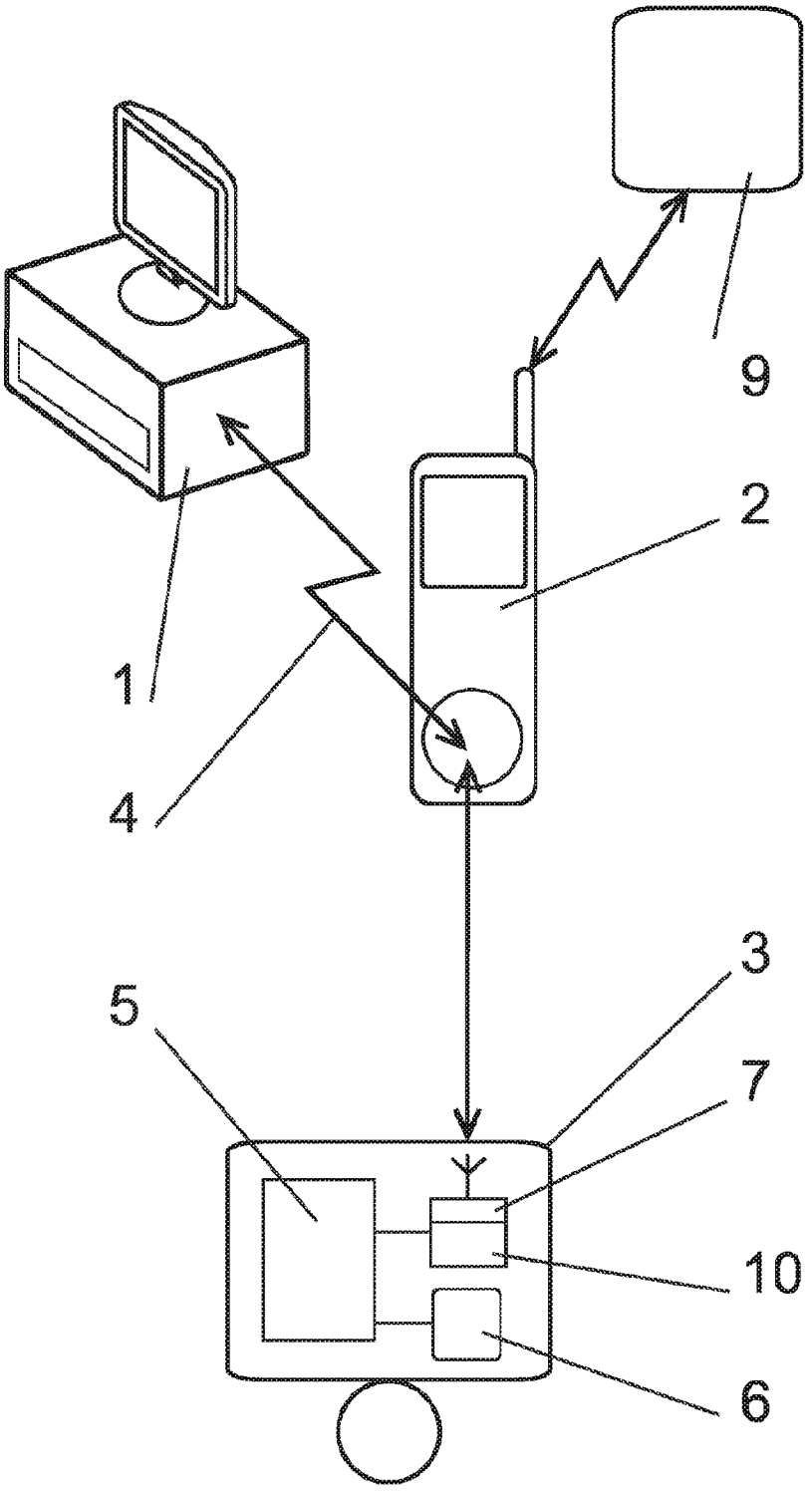


Fig. 2

SYSTEMS AND METHODS FOR CONTACTLESS PAYMENT AUTHORIZATION

FIELD OF INVENTION

[0001] The invention relates to a method and a system of authenticity of authorized persons and transaction approval, particularly at direct debits (noncash payment system) by means of a mobile communication device, principally a mobile phone connected to a payment terminal where the mobile communication device functions as a payment card. The invention also concerns an identifier, used for authentication and manipulation, due to which the approval with the operation, principally payment transaction is indicated.

PRESENT TECHNOLOGY STATUS

[0002] Debit cards, of which the payment confirmation is made by its submitting and entering the correct PIN, are frequently used by direct debits. Very often the direct debit is realized in such way that the purchaser at the payment submits the payment card to the trader who inserts it in the terminal and asks the purchaser to agree the total sum of the purchase. The purchaser enters, mostly with the small keyboard, the PIN into the terminal and the payment is confirmed. By means of PIN the purchasers authenticate themselves at the payment via magnetic, chip or contact free (RFID) payment cards and also at the payments by mobile phones when the act of payment can by done by means of payment terminals or mobile banking direct payments.

[0003] Known are more methods and technical means which substitute manual PIN entering in the mobile phone and also by which the confirmation of the direct debit is made. For example according to the published PCT application form WO 2005/086456 A1, RFID chip is used in a small movable card located separately from the mobile phone. RFID technology is described also in patents and patent registrations: EP 1 536 573 A2, CN 1627321 A, KR20040060249, WO 2007/136939 A2, WO 2006/009460 A1. However, RFID chip was developed for applications with a lower level of security such as pallet monitoring in a warehouse, input and distribution of the goods et cetera. RFID technology does not enable the active cryptography of to be approved alphanumerical chain neither without a contact connection between the RFID identifier and the source nor without the use of the own energy source like battery. The use of NFC technology is known also in patents and patent registrations: EP 1 729 253 A1, DE 10 2006 019 628 A1, CN 1835007. However, known is no solution, by which the passive identifier is used without own energy source but making cryptographic operations itself.

[0004] Until now known methods and devices did not ensure sufficiently high level of security with passive identifiers, since they can be copied and imitated easily. Active identifiers, on the other hand, demand the own energy source able to supply the hardware of the identifier by energy needed for cryptography of the approving code or a contact connection to a communication device to supply with the energy. However, both methods are uncomfortable and time-consuming.

BACKGROUND TO INVENTION

[0005] Disadvantages mentioned above are eliminated significantly by the method of authenticity and/or agreement approval at the direct debits through the separate identifier according to this invention, of which bedrock is based on the fact that after activating the payment process or payment process preparation in the mobile communication device, the device sends alphanumerical chain into the identifier approached to the mobile communication device. The identifier is approached in the distance shorter than 10 cm, mostly it may touch the mobile communication device directly. However, the contact or the contact point setting is not essential or necessary since the communication between the mobile communication device and the identifier is wireless. At this point, the identifier is by means of energy supplied contact free from the electromagnetic field of the mobile communication device, receives alphanumerical chain and realizes its processing in the form of an electronic signature. The received alphanumerical chain is signed electronically in the identifier and such established signed alphanumerical chain is sent back to the mobile communication device where the correctness is checked. If the correctness is verified and at the same time the owner approves the payment transaction, the mobile communication device will be approached to the distance, suitably less than 10 cm from the reading unit of the payment terminal.

[0006] It is advantageous if the electronic signature of the received alphanumerical chain is made by the process with the help of a private key saved in the memory of the identifier. To the energy supply of the identifier circuits is used direct and/or while approaching, accumulated energy of the electromagnetic field of the mobile communication device, advantageously electromagnetic field created by transmitting unit of the mobile communication device which aim is to communicate with the identifier.

[0007] The invention enables to use cryptography of the authentication preserving the energy passivity of the separate identifier. The principal advantage is the high level of security at the satisfactory user comfort. Entering PIN code mostly consisting of four digits can be according to this invention, replaced by apposing the identifier working with more-bit-chain which is variable since the approving code transmitted from the identifier into the mobile communication device is changed according to the cryptography taking place in the identifier processor at every authentication process. By this, the higher level of security is achieved than at the RFID identifiers and the advantage of its passivity is remained. Such energy passivity enables to reduce the size of the identifier since there is no necessity to use own energy source by which the user comfort is increased as the user does not have to bother with identifier's charge or condition.

[0008] In a favorable configuration the mobile communication device may use at the payment processing and authentication a remote processing server to which it is connected via general mobile network, mainly the kind of GSM or GRPS net.

[0009] The bedrock of this invention is based on the system of authentication and/or agreement approval at the direct debits which concerns payment terminals, a separate identifier and a mobile communication device communicating with the payment terminal via contact free communication channel where the mobile communication device, preferably mobile phone, contains transmitting and receiving unit to allow the contact free communication with the identifier and where the identifier contains a processor for electronic signature of the received alphanumerical chain. Further more, the identifier contains transmitting and receiving unit to allow the communication with the mobile communication device, a block transforming the electromagnetic field into the electric

energy and a memory. Components of the identifier are, from the energy point of view, supplied by electromagnetic field of the mobile communication device either directly by immediately gained energy or partially by energy accumulated during the approaching to the mobile communication device at the relevant payment process.

[0010] In a possible configuration the system includes a remote processing server connected to the mobile communication device through general mobile network, preferably via GSM or/and GPRS net. From the point of view of compatibleness with the existing, mass-spread devices and standards, it is suitable if the mobile communication device consists of a mobile phone, advantageously a mobile phone with NFC communication unit.

[0011] Disadvantages mentioned in the Present Technology Status are eliminated significantly by the identity identifier and/or agreement approval at the direct debits through communicating contact free with the mobile communication device, principally a mobile phone which is connected contact free to the payment terminal according to this invention, of which bedrock is based on the fact that it consists of a processor for electronic signature of the received alphanumerical chain, transmitting and receiving unit to communicate with the mobile communication device. Communication is principally based on receiving the alphanumerical chain and transmitting electronically signed alphanumerical chain. The identifier further more contains a memory, a block transforming the electromagnetic field into the electric energy. Transmitting and receiving unit and a block transforming the electromagnetic field into the electric energy are connected to the processor. Processor is also connected to the memory. Basically, all the units of the identifier are, from the energy point of view, supplied by electromagnetic field of the mobile communication device.

[0012] In an advantageous configuration, the identifier of identity and/or approval contains NFC chip and the memory contains a private key for electronic signature of alphanumerical chain received from the mobile communication device.

[0013] Utility attributions increase a configuration, where a part of the memory is reserved for the personal data of the user. This part of memory is adjusted to store the personal user data separately from the private key. In such case the identifier may be used like a health insurance card, identity card and so on. Rightness of data demand is evaluated in the processor of the identifier.

[0014] To increase the user comfort, the identifier may be located in a pendant and/or a key ring and/or a label and/or a beading.

[0015] The invention enables to higher the level of security and comfort of authenticity and direct debit approval since the user does not have to remember his PIN code. At the same time the invention increases the process of direct debit transaction since the mobile communication device functions as a wallet without any delay caused by the PIN code entering.

DESCRIPTION OF DRAWINGS

[0016] The invention is described in more details by means of pictures **1** and **2**, where picture **1** shows the connection scheme of a payment terminal, a mobile communication device and an identifier at the direct debit transaction.

[0017] Picture **2** represents the scheme of connection between payment terminal, identifier and mobile communication device associated with a remote server at the direct debit transaction.

EXAMPLES OF APPLICATION

Example 1

[0018] In this example the system contains a payment terminal **1** located at the cash register in a shop, a mobile communication device **2** represented by a mobile phone NOKIA 6131 serially equipped by NFC technology and an identifier **3** situated in a key ring.

[0019] The payment terminal **1** allows contact free radio communication with the mobile communication device **2** while the payment terminal **1** is of a common standard with usual functions and communication with payment servers at the bank central office or other similar institution such as authorized centers.

[0020] Mobile communication device **2**, herein NOKIA 6131, functions as a payment card in such way that it contains in its memory a software application which enables to realize the payments in cooperation with the payment terminal **1**. Needed data are sent via air from the mobile communication device **2** into the payment terminal **1** after the activation of the necessary payment process and approaching the mobile communication device **2** to the payment terminal **1**, actually to NFC reader of the payment terminal **1**.

[0021] Mobile communication device **2** allows a safe and correct recording and storing of the payment software application in a secured memory and has the ability to realize contact free radio communication between the payment terminal **1** and the identifier **3**.

[0022] At the payment, except for approaching the mobile communication device **2** to payment terminal **1**, it is needed to authenticate, approve the presence of the user at the payment and to confirm his agreement with the payment. To authentication and payment confirmation is used an identifier **3** containing a processor **5**, which beside recording memory with the private key, is able to realize computationally operations which enable cryptography and decryption needed for electronic signature realization. The identifier **3** does not contain its own energy source (f.e. battery) and uses as energy source the electromagnetic field of the mobile communication device **2** which is processed in a block **10** of transformation. The identifier **3** is able to communicate with the external devices, principally mobile communication device **2**, possibly the payment terminal **1** or programming devices, exclusively contact free via radio transmission.

[0023] The payment approval is given in such way that the mobile communication device **2** is either approached or directly put close to the identifier **3** in distance shorter than 10 cm, by which the alphanumerical chain is transmitted into the identifier **3**. The identifier **3** receives the chain and signs it electronically by a private key and such signed alphanumerical chain sends back into the mobile communication device **2**. These operations are completed by processing in a circuit of the identifier **3** via energy from the electromagnetic field of the mobile communication device **2**. Receiving the correct alphanumerical code from the identifier **3** into the mobile communication device **2**, the payment application of the mobile communication device **2** considers that the user approved the payment and that the user is authorized.

[0024] Correctness verification is basically reading of the electronically signed alphanumerical code via particular general key. Later the user approaches the mobile communication device **2** to the payment terminal **1**, by which the payment process will be agreed in the payment terminal **1** from where the payment data are sent in a standard way to the bank or authorized centre. In a common practice, the payment transaction may be realized in such way that the user, while waiting at the cash desk activates in his mobile phone the payment process or preparation for this process. The user chooses from the menu on his display the account he wants the payment to be realized from and puts the identifier **3** closer to the mobile phone. The user, after the receipt is printed by the cash register, decides if he wants to pay the amount and if yes, the user approaches the mobile phone to the payment terminal **1**, technically to its reading unit which is marked graphically. The payment terminal **1** prints out the receipt or according to the setting, the user receives SMS about the realized payment. This way the direct debit process will be speed up significantly.

[0025] In this example is a part **8** of the memory **6** reserved for the personal data of the user and the identifier **3**, in a connection to a suitable reading unit of NFC chip, may be used as electronic ID, health insurance card and so on. Different kinds of such personal data are accessible by means of various levels of access rights evaluated by the processor **5**.

Example 2

[0026] Example 2 differs from the above mentioned one in the way that the configuration contains a remote server **9** processing the payment transactions which are therein realized directly in the mobile communication unit **2**. In this example the mobile communication device **2** works as a processing mediator and shows the processes which are realized in a distance as a viewer. The connection is made via GPRS data network.

INDUSTRIAL APPLICABILITY

[0027] Industrial applicability is obvious. According to this invention, it is possible to authenticate and approve the direct debit processes industrially and repeatedly, principally via a mobile phone with the use of a passive identifier.

[0028] According to this invention it is also possible to produce and use passive identifiers, principally by using NFC chip standards where the source, according to this invention, may be supplied by the electromagnetic field of the mobile communication device. The invention is also related to identifier which functions to authentication and approval indication and as well it may be used as a kind of personal cards.

LIST OF RELATED SYMBOLS

[0029] **1**—payment terminal
[0030] **2**—mobile communication device
[0031] **3**—identifier
[0032] **4**—contact free communication channel
[0033] **5**—processor
[0034] **6**—memory
[0035] **7**—transmitting and receiving unit
[0036] **8**—part of memory used for personal data
[0037] **9**—remote server
[0038] **10**—block of transformation

1-8. (canceled)

9. A method for contactless payment authorization, the method comprising:
- initiating a payment process in a mobile communication device;
- communicating an alphanumeric string from the mobile communication device into an identifier located sufficiently near to the mobile communication device such that the identifier is supplied with energy from an electromagnetic field of the mobile communication device;
- electronically signing the received alphanumeric string in the identifier;
- sending the electronically signed alphanumeric string to the mobile communication device;
- verifying the electronically signed alphanumeric string in the mobile communication device; and
- placing the mobile communication device sufficiently near to the payment terminal to realize a payment.

10. The method of claim **9**, further comprising locating the identifier within ten centimeters of the mobile communication device.

11. The method of claim **9**, further comprising placing the mobile communication device within ten centimeters of the payment terminal to realize the payment.

12. The method of claim **9**, wherein the mobile communication device is a mobile telephone.

13. The method of claim **9**, wherein the mobile communication device is connected to a remote processing server through a public mobile network, and the mobile communication device uses the remote processing server for payment processing and/or authentication.

14. The method of claim **9**, wherein the mobile communication device includes a near-field communication element that generates the electromagnetic field.

15. The method of claim **9**, wherein the identifier comprises a memory that contains a key for use in electronically signing the received alphanumeric string, and wherein the received alphanumeric string is electronically signed in the processor using the key.

16. The method of claim **9**, wherein mobile communication device comprises a receiving element for communication with the identifier, and wherein the electromagnetic field is generated by the receiving element.

17. A system for contactless payment authorization, the system comprising:
- an identifier; and
- a mobile communication device that communicates with a payment terminal over a near-field communication channel,
- wherein the mobile communication device is equipped with a transmitting and receiving element for contactless communication with the identifier, and
- wherein the identifier is supplied with electrical energy from an electromagnetic field of the mobile communication device and comprises a processor for electronically signing a received alphanumeric string, a transmitting and receiving element for communication with the mobile communication device, a block for transforming the electromagnetic field into the electrical energy, and a memory.

18. The system of claim **17**, wherein the memory contains a stored identification number and a key for use in electronically signing the received alphanumeric string.

19. The system of claim **17**, wherein the transmitting and receiving element in the mobile communication device and the transmitting and receiving element in the identifier are near-field communication units.

20. The system of claim **17**, wherein the mobile communication device is a mobile phone.

21. The system of claim **17**, wherein the mobile communication device is connected to a remote processing server through a public mobile network, and the mobile communication device uses the remote processing server for payment processing and/or authentication.

22. The method of claim **21**, wherein the remote processing server is a Global System for Mobile communications (GSM) or General Packet Radio Services (GPRS) server.

23. An identifier for use in a contactless payment authorization system, the identifier for use with a mobile communications device in contactless communication with a payment terminal, the identifier comprising:

a processor for electronically signing an identifying code received from the mobile communications device;

a transmitting and receiving unit for communicating with the mobile communication device, the transmitting and receiving unit for receiving the identifying code and transmitting the electronically signed identifying code;

a memory that contains a stored identification number and a key for use in electronically signing the received identifying code;

a block for transforming an electromagnetic field of the mobile communication device into electrical energy that is supplied to the processor, the transmitting and receiving unit, and to the memory.

24. The identifier of claim **23**, wherein the memory contains a private key for use in electronically signing the identifying code.

25. The identifier of claim **23**, further comprising a near-field communication unit.

26. The identifier of claim **23**, wherein at least a portion of the memory is configured for separately storing personal data associated with a user.

27. The identifier of claim **26**, wherein the portion of the memory that is configured for separately storing the personal data is externally accessible via the transmitting and receiving unit.

28. The identifier of claim **23**, wherein the identifier is located in a pendant, a key ring, a label, or an applique.

* * * * *