



(51) International Patent Classification:
G06Q 30/00 (2006.01)

(21) International Application Number:
PCT/EP2010/070540

(22) International Filing Date:
22 December 2010 (22.12.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09291004.1 31 December 2009 (31.12.2009) EP

(71) Applicant (for all designated States except US):
GEMALTO SA [FR/FR]; Intellectual Property Dpt, 6
rue de la Verrerie, F-92190 Meudon (FR).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **GRENIER, Fabrice**
[FR/FR]; c/o Gemalto SA, Intellectual Property Dpt, 6 rue
de la Verrerie, F-92197 Meudon Cedex (FR).

(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, 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, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG,
ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

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

(54) Title: METHOD FOR PROVIDING AN ELECTRONIC RECEIPT

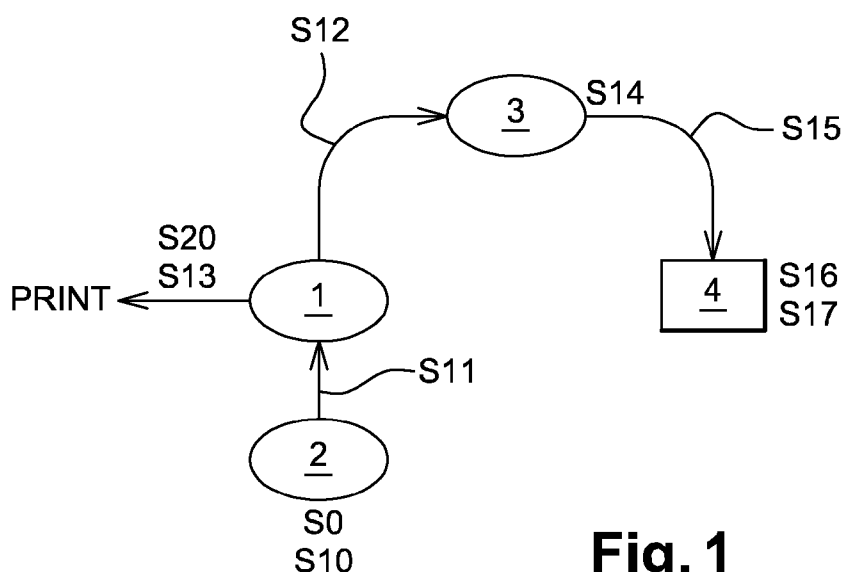


Fig. 1

(57) Abstract: The present invention is a method for providing, to a user (4), a receipt transacted at a point-of-sale device with a secure device of said user (4), wherein it (step S0) storing a destination of the user (4), a destination of a trusted service (3) and a public key of the trusted service (3), sending securely at the destination of the user (4) said electronic receipt by the point-of-sale device, wherein the destination of the user (4) is encrypted with the public key of the trusted service (3) (step S10).

METHOD FOR PROVIDING AN ELECTRONIC RECEIPT**FIELD OF THE INVENTION**

5 The invention relates to the field of commercial transactions, and especially deals with electronic transactions.

BACKGROUND OF THE INVENTION

Point-of-sale (POS) devices are widely used for processing
10 transactions. Banks and Merchants are always complaining of paper roll management and cost of these paper rolls. Banks mention as an issue the stock management of paper roll, especially when they have different diameters.

In some countries, banks and merchants would like to perform
15 transactions without providing a ticket receipt to the cardholder.

The document US2007006901 proposes an electronic equipment which performs a transaction that may ask the cardholder what he wants to do with the transaction. In this case, the user can choose to store the electronic receipt on a smart card or to send it sent to
20 an email address which can be specified by the cardholder manually.

Nevertheless in this method, the cardholder has to enter his personal data into the terminal of the merchant which is not secure.

2

SUMMARY OF THE INVENTION

It is an object of the invention to provide a new way for preventing ticket receipt printing after each transaction, by sending to the cardholder the electronic receipts in a secure manner so as to avoid using paper and to receive details of the transactions securely and without giving to the point-of-sale the destination of the cardholder.

Thereto, the present invention provide a method for providing, to a user, a receipt transacted at a point-of-sale device with a secure device of said user, wherein it comprises storing a destination of the user, a destination of a trusted service and a public key of the trusted service, sending securely at the destination of the user said electronic receipt by the point-of-sale device, wherein the destination of the user is encrypted with the public key of the trusted service.

According to other aspects of the invention:

- once the destination of the user has been encrypted and after a transaction has been operated, the secure device may send the encrypted destination of the user and the destination of the trusted service to the point-of-sale device;
- it may comprise sending the receipt and the encrypted destination of the user to the trusted service;

3

- the trusted service may decrypt the user destination with its private key so as to send the receipt to the destination of the user;
- the trusted service may receive a receipt delivery when the receipt is successfully received by the user;
- it may comprise printing the receipt if the sending of the receipt and the encrypted destination of the user to the trusted service fails or if the sending of said receipt to the destination of the user is unsuccessful;
- the transaction between the secure device and the point-of-sale device may be done contactless;
- it may comprise signing the encrypted destination of the user;
- it may comprise sending the signed encrypted destination to the trusted service;
- it may comprise storing a counter value which increases at each transaction or means a random value which is generated at each transaction, said counter value or said random value being used for a concatenation with the destination of the user before being encrypted and/or signed by said secure device;
- it may comprise encrypting the receipt;
- it may comprise storing a public key of the user and storing a private key of the user associated with said public key of the user, said public key of the user being used for encrypting the receipt;

4

- it may comprise updating the destination of the user or the trusted service in the secure device of the user.

Thanks to this method, an email address of the cardholder and a public key are stored in the card during the personalization of the card. It provides storing email address of a cardholder in a secure device such as a smart card, sending to himself an email address without providing the email address to sending machine, and securing the content of an email sent to himself so as to be the only one able to read that email.

Thanks to this method, a cardholder can easily store directly only desired transactions received by email. The cardholder is the only person who can open and read the electronic receipt.

The destination for the reception of the receipt is not known by the POS device.

The cardholder can be the only person who can open and read the receipt. No one else being able to know which product or service has been purchased

The use of a trusted service avoids to a cardholder to give his mail address and therefore avoid to be spammed from the sender, or any other third party. Only the trusted service can access the card holder email address.

5

The invention is now described, by way of example, with reference to the accompanying drawings. The specific nature of the following description should not be construed as limiting in any way the broad nature of this summary.

5

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the manner in which the above recited and other advantages and features of the invention are obtained, a more particular description of the invention briefly described above will
10 be rendered by reference.

Notwithstanding any other forms that may fall within the scope of the present invention, preferred forms of the invention will now be described, by way of example only, with reference to the accompanying drawing in which:

15 **FIG.1** schematically shows an embodiment of a method according to the invention in a nominal use case.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention may be understood according to the detailed description provided herein.

20 Shown in Fig.1 is an embodiment of the method according to the invention for electronically receipting transactions transacted at a terminal such as a POS device 1.

6

The POS device 1 is adapted to send electronic transactions.

When a user 4 or a cardholder 4 goes to the merchant and purchases some goods, the merchant first enters a corresponding amount in a terminal 1 or point-of-sale device 1 (POS).

5 The cardholder 4 or the merchant then enters a secure device 2 such as a card 2 of the cardholder in a corresponding slot of the terminal and for example enters a PIN code.

10 The card stores classical data associated to the account of the cardholder 4 such as his account number, his name, a date of validity, etc...

15 In the following description, the POS device 1 is able to provide electronic receipts and the cardholder accepts automatically to receive by email the electronic receipts of the transactions he made. It is well understood that if there is no cardholder mail address stored in the card, the POS device 1 prints automatically the receipt.

 According to the invention, in a step S0, the card stores the destination of the user, a destination of a trusted service 3 and a public key of the trusted service 3.

20 The destination of the user or cardholder 4 is the mail address of the cardholder 4, and the destination of the trusted service 3 is the mail address of the trusted service 3.

 The mail address and the public key of the trusted service 3 are provided by the bank of the cardholder 4.

25 All these data are stored at the personalisation of the card.

7

In a step S10, the mail address of the cardholder 4 is encrypted with the public key of the trusted service 3.

Once the mail address has been encrypted in step S10, and after a transaction has been operated, in a step S11, the card sends the encrypted mail address of the cardholder 4, and in clear the mail address of the trusted service 3 to the POS device 1.

In a step S12, the POS device 1 sends the receipt corresponding to the transaction that has been operated and the encrypted mail address to the trusted service 3. The POS device 1 uses the address mail of the trusted service 3.

In a step 13, the receipt is printed by the POS if the sending to the trusted service fails, which may for example happen when the connection between the POS and the trusted service 3 fails, for example due to a sending to a wrong mail address of the trusted or due to an interruption of the connection.

In step S14, the trusted service 3 decrypts the cardholder 4 mail address with its own private key.

Then in a step S15, the trusted service 3 sends the receipt to the address mail of the cardholder 4 it has decrypted. Then In a step S17, the cardholder 4 consults the mailbox corresponding to the mail address stored in his card, and can read and treat his receipt.

In these steps, the receipt is sent enclosed to a classical mail to the trusted service and to the cardholder 4.

In another embodiment, after the step S15, when the cardholder 4 successfully receives a message in the mailbox corresponding to the

8

mail address stored in his card and decrypted by the trusted service 3, in a step S16, a receipt delivery is sent to the trusted service 3. Otherwise, if in step S15 the sending of the receipt by the trusted service 3 to the mail address of the cardholder 4 is unsuccessful, the POS prints a receipt in a step 20. This may for example happen if the mail address of the cardholder 4 is not valid. In this case, the trusted service 3 receives an error message. The trusted service 3 send back this message or a corresponding flag to the POS device 1 for printing the receipt.

10

In another embodiment, in step S0, a private key of the bank of the cardholder 4, provided by the bank of the cardholder 4, is stored in the card. A public key of the bank associated with this private key, is sent by the bank of the cardholder 4 to the trusted service 3 in which it is then stored. The private key of the bank is used by the card to sign, in a step S21, the encrypted mail address of the cardholder 4. The public key of the bank is used by the trusted service for checking the signature when it receives the encrypted mail address by the POS.

20

The private key of the bank can also be used to sign the stored mail address of the cardholder 4 only without any encryption.

25

In another embodiment, in step s0, the card stores a counter which increases at each transaction or means adapted to generate a random number which generate a random number at each transaction. The mail address is concatenated with the counter value or with the

9

random value. The concatenated data is then encrypted with the private key of the trusted service 3.

The concatenated data or the random value or the counter value is signed by the card. The signature is then different for each transaction. When receiving the encrypted data, the trusted service 3 checks the signature using the public key of the bank of the cardholder 4, and can advantageously prove to the bank of the cardholder 4 how many services it has really performed in order to charge the bank for the provided service(s). Of course it is well understood that the trusted service has to provide also how many receipt he really sends to the cardholder 4 by providing to the bank for example a copy of the messages sent to the cardholder 4, or a copy of delivery receipts, etc..

With these embodiments, the card can send to the POS device 1, in step S11, the mail address of the user which is encrypted and signed, or the mail address of the cardholder 4 encrypted and the mail address of the cardholder 4 signed, or both the mail address of the cardholder 4 and the value of the counter encrypted and signed, or both the mail address of the cardholder 4 and the value of the counter encrypted and the mail address of the cardholder 4 signed.

In another embodiment, the card of the cardholder 4 stores a public key of the cardholder 4 for encrypting the receipt. In the step S11, the card may also sends the public key of the cardholder 4 to the POS device 1 so as the POS device 1 is able to encrypt the

10

receipt with this key. The receipt is encrypted in the POS device 1 before being sent for example as an enclosed document, to the trusted service 3. The POS device 1 may include an algorithm of encryption, and uses the public key of the cardholder 4 received by the card. The cardholder 4 has an associated private key for the decryption of the encrypted receipt. Only the cardholder 4 can advantageously decrypt the receipt with its private key. Neither the trusted service 3 nor someone who would have intercepted or tried to read the message of the cardholder 4, can know details of the transaction.

10

In another embodiment, the receipt is encrypted in the trusted service 3 before being sent to the cardholder 4. In this case, the POS 1 also sends to the destination of the trusted service, the public key of the cardholder 4 provided by the card of the cardholder 4 with the receipt and the encrypted and/or signed data which comprises the mail address of the cardholder 4. The cardholder 4 can then decrypt the receipt with its private key.

15

In another embodiment, the receipt is sent as part of the mail the trusted service or the cardholder 4 will receive respectively from the POS device 1 or the trusted service 3.

20

In this case, the message can be encrypted. For doing so, the trusted service 3 and a terminal of the cardholder 4 used for reading his emails, embeds specific softwares for mail encryption and decryption. They can use standard solutions as known in the art for the encryption and the decryption such as S_MIME, openPGP, etc...

25

In another embodiment, after step 16, the trusted service 3 sends in its turn the delivery receipt to the POS device 1 so as the POS device 1 is able to detect if the electronic receipt has been successfully been received. The POS may display a message which informs the cardholder 4 that data related to the transaction have been sent by email in a step S19, which can then be checked by the cardholder 4.

10 According to the present invention, the POS prints the receipt if any problem occurs during the processing of reading the card.

The POS device 1 may also print a receipt if no message is received from the trusted service 3 within a predetermined time period, for example if the trusted service does not receive any delivery receipt.

15 The POS device 1 may also print a receipt if no message is received by the cardholder 4 at the end of a predetermined time, for example at the end of 1 minute. The cardholder 4 in this case is able to check the reception of the receipt using for example a mobile phone.

20 In another embodiment, the transaction between the secure device and the terminal is done contactless. The POS is equipped with a contactless reader able to exchange data with contactless secure devices (dual interface card, pure contactless card, NFC a Near-Field

12

Communication (NFC) enabled mobile handset or other type of contact or contactless communication.

5 According to another embodiment, it is possible to update the destination of the trusted service 3 and the associated key. It is also possible to update the destination of the cardholder 4 or to have more than one trusted service or destination of the cardholder 4 that can be selected by the card or the POS.

10

 If POS is for example corrupted and sends voluntarily the electronic receipt to a fake trusted service, it is accepted that the ticket will not be printed, the fake trusted service will not be able to decrypt the email address of the cardholder and the cardholder
15 will never receive its electronic email.

 It will be well understood that all these embodiments can be combined and are not limited examples, and that anyone who wants to receive securely a transaction or any message from a point-of-sale
20 service or any sender service without giving this sender service the destination address can use this secure method.

 Thanks to the invention the email address is securely stored in the smart card which provides a public key to secure the receipt
25 sending. The use of a trusted service avoids to a cardholder to give his mail address and therefore avoid to be spammed from the sender,

or any other third party. Only the trusted service can access the cardholder email address.

14
CLAIMS

- 5 1. Method for providing, to a user (4), a receipt transacted at a point-of-sale device with a secure device of said user(4), wherein it comprises (step S0) storing a destination of the user (4), a destination of a trusted service (3) and a public key of the trusted service (3), sending securely at the destination of the
- 10 user (4) said electronic receipt by the point-of-sale device, wherein the destination of the user (4) is encrypted with the public key of the trusted service (3) (step S10).
2. Method according to claim 1, wherein once the destination of the
- 15 user (4) has been encrypted (step S10) and after a transaction has been operated, the secure device sends (step S11) the encrypted destination of the user (4) and the destination of the trusted service (3) to the point-of-sale device.
- 20 3. Method according to claim 2, wherein it comprises sending (step S12) the receipt and the encrypted destination of the user (4) to the trusted service (3).
4. Method according to claim 2 to 3, wherein the trusted service (3)
- 25 decrypts (step 14) the destination with its private key so as to send (step 15) the receipt to the destination of the user(4).

15

5. Method according to claim 4, wherein the trusted service (3) (step S16) receives a receipt delivery when the receipt is successfully received by the user (4).

5 6. Method according to claim 3 or 4, wherein it comprises printing (step S13, S20) the receipt if the sending (step S12) of the receipt and the encrypted destination of the user (4) to the trusted service (3) fails or if the sending (step S15) of said receipt to the destination of the user (4) is unsuccessful.

10

7. Method according to one of the previous claims, wherein the transaction between the secure device and the point-of-sale device is done contactless.

15 8. Method according to one of the previous claim, wherein it comprises signing (step S21) the encrypted destination of the user (4).

9. Method according to claim 8, wherein it comprises sending the
20 signed encrypted destination to the trusted service (3).

10. Method according to one of the previous claim, wherein it comprises storing a counter value which increases at each transaction or means a random value which is generated at each
25 transaction, said counter value or said random value being used

16

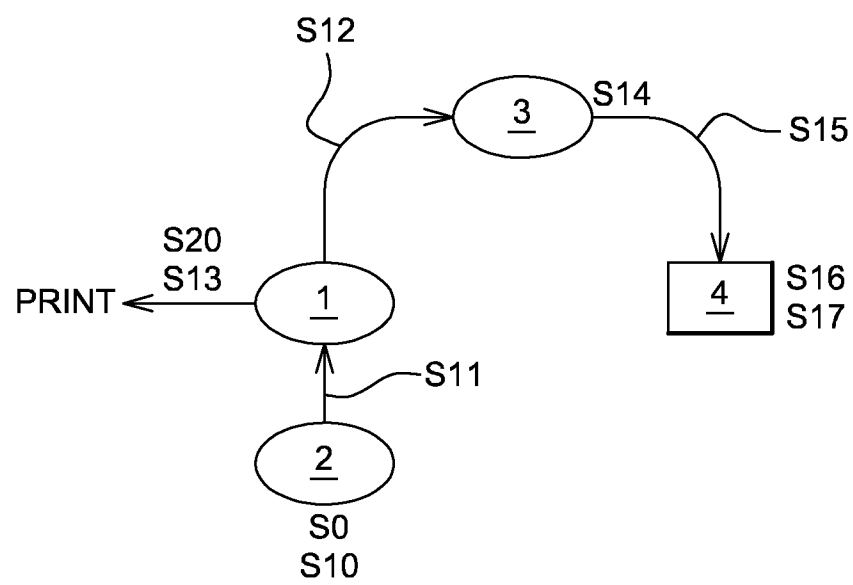
for a concatenation with the destination of the user (4) before being encrypted and/or signed by said secure device.

11. Method according to one of the previous claim wherein it
5 comprises encrypting the receipt.

12. Method according to claim 11, wherein it comprises storing a
public key of the user (4) and storing a private key of the user
(4) associated with said public key of the user (4), said public
10 key of the user (4) being used for encrypting the receipt.

13. Method according to one of the previous claim, wherein it
comprises updating the destination of the user (4) or the trusted
service in the secure device of the user (4).

1/1

**Fig. 1**

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2010/070540

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06Q30/00

ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

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 practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
L	"STATEMENT IN ACCORDANCE WITH THE NOTICE FROM THE EUROPEAN PATENT OFFICE DATED 1 OCTOBER 2007 CONCERNING BUSINESS METHODS - EPC / ERKLAERUNG GEMAESS DER MITTEILUNG DES EUROPAEISCHEN PATENTAMTS VOM 1.OKTOBER 2007 UEBER GESCHAEFTSMETHODEN - EPU / DECLARATION CONFORMEMENT AU COMMUNIQUE DE L'OFFICE EUROP", JOURNAL OFFICIEL DE L'OFFICE EUROPEEN DES BREVETS.OFFICIAL JOURNAL OF THE EUROPEAN PATENT OFFICE.AMTSBLATTT DES EUROPAEISCHEN PATENTAMTS, OEB, MUNCHEN, DE, 1 November 2007 (2007-11-01), pages 592-593, XP007905525, ISSN: 0170-9291 Statement in accordance with the Notice from the European Patent Office dated 1 October 2007 concerning business methods(OJ 11/2007; p592f) The claimed subject matter, with due	1-13



Further documents are listed in the continuation of Box C.



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 document 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

27 January 2011

Date of mailing of the international search report

04/02/2011

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Tiago Pinheiro

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/070540

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	regard to the description and drawings, relates to processes comprised in the list of subject matter and activities excluded from patentability under Art.52(2) and (3) EPC. The applicant is advised that in accordance with the established practice of the EPO, no search need be performed in respect of those aspects of the claimed invention. The only identifiable technical aspects of the claimed invention relate to the use of conventional, general-purpose data processing technology for processing data of an inherently non-technical nature. The information technology employed is considered to have been generally known as it was widely available to everyone at the date of filing/priority of the present application. The notoriety of such prior art cannot reasonably be contested. No documentary evidence was therefore considered required. -----	