



(51) International Patent Classification:

G06Q 20/30 (2012.01) G06Q 20/40 (2012.01)  
G06Q 20/32 (2012.01)

(21) International Application Number:

PCT/EP2017/000921

(22) International Filing Date:

28 July 2017 (28.07.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16001691.1 01 August 2016 (01.08.2016) EP

(71) Applicant: GIESECKE+DEVRIENT MOBILE SECURITY GMBH [DE/DE]; Prinzregentenstr. 159, 81677 München (DE).

(72) Inventor: KÄHKÖNEN, Mikko; Thalkirchner Strasse 31, 80337 München (DE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: WIRELESS PAYMENTS USING A WEARABLE DEVICE

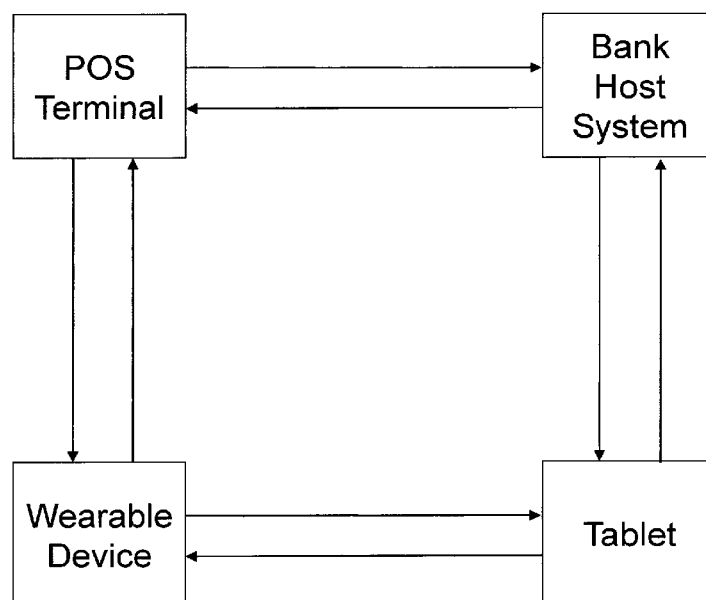


Fig. 2

(57) Abstract: The present invention is directed towards a method for securely performing wireless payments being triggered by a wearable device, which can be performed efficiently regarding hardware requirements. The present invention is further directed towards a communication protocol implementing the suggested method steps as well as a system for performing secure wireless payments using a wearable device. The invention is furthermore directed towards a computer program product comprising instructions implementing the suggested method steps and operating the suggested system.



**Declarations under Rule 4.17:**

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

**Published:**

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

### Wireless Payments Using a Wearable Device

5 The present invention is directed towards a method for securely performing wireless payments being triggered by a wearable device, which can be performed efficiently regarding hardware requirements. The present invention is further directed towards a communication protocol implementing the suggested method steps as well as a system for performing secure wireless payments using a wearable device. The invention is furthermore directed to-  
10 wards a computer program product comprising instructions implementing the suggested method steps and operating the suggested system.

US 2014 052640 A1 shows a method of establishing security and authentication credentials for secure communication between a wallet service center  
15 and a cluster of electronic wallet transaction facilities provided at a user device.

According to the prior art newly developed computer devices are provided,  
20 which are implemented using a minimum of hardware capacities. So-called wearable devices are computing devices of every day's life which are enhanced by a microprocessor and respective memories. This may be suitable for tracking fitness exercises such as jogging, where a pulse rate is detected. Typically such devices are of light weight as they need to be carried around  
25 by the user all the day. Consequently, such devices hold only a minimum of components at least for the comfort of the user.

A further aspect of such commonly known devices is that they must not be highly power consuming as the respective battery is typically of low capacity  
30 and needs to be charged every day or at least every second day. Hence, there

- 2 -

is a requirement for efficiently implementing such hardware devices comprising only a specific number of components which are essential for providing the required functionality.

- 5 These wearable devices are typically manufactured in large capacities at a reasonable price. This also leads to the conclusion that only those components being effectively required are to be provided by the manufacturer. In case additional components would be involved the weight as well as the energy consumption would rise. Consequently, there are several application domains which cannot be handled by such known devices. To be able to address each and every application domain such mobile devices would have to comprise every thinkable component for getting involved in every application scenario. Consequently, such devices are specifically tailored to single application domains, such as fitness tracking for instance. Consequently, all components being not required for fitness tracking are omitted in such devices.

Commonly known methods apply mobile devices for user authentication. Such an authentication process may be performed using biometric sensors.

- 20 For instance, it is commonly known to provide a fingerprint to a smartphone identifying the respective user. Such a provided fingerprint is compared to a further stored fingerprint and thereupon a device can be unlocked. However, there is a disadvantage as for such an application an additional fingerprint sensor needs to be applied. Such a sensor at least raises the manufacturing costs for the mobile phone.

The payments industry is increasingly looking into solutions for making innovative wearable devices available for cardholders to make contactless proximity payments. In pursuing options for this goal, many institutions are

- 3 -

raising questions about managing the expenditure particular in environments where online authorization is not possible, as well as expressing concerns above the fact that these transactions are carried out without any cardholder verification. A wearable device typically has no feature allowing for  
5 cardholder verification, and contactless payment terminals typically do not cater for reception of an authorization response which could reset expenditure counters in the payment application in a wearable device.

A further application of the solution could be to use the biometric as a user  
10 verification method for large ticket purchases, to be paid by a wearable device.

Consequently, it is an object of the present invention to provide a method which allows a wearable device to take part in several application domains  
15 without requiring a large variety of hardware components. Accordingly, such a device shall only be composed of a minimum of components leading to low manufacturing costs and low energy consumption. It is furthermore an object of the present invention to provide a respective communication protocol along with a system for performing secure payments by means of a  
20 wearable device. It is further an object of the present invention to provide a respective computer program product.

The object is solved by a method comprising the subject matter of independent claim 1. Further advantages are provided by the dependent claims.  
25

Accordingly, a method for performing secure wireless payments using a wearable device is suggested. The method comprises the steps of triggering a payment transaction wirelessly by the wearable device, whereupon a transaction request and an authentication request is transmitted from a payment

- 4 -

terminal to the wearable device, whereby a verification metric is provided indicating whether the following steps are to be performed. Namely, forwarding at least the authentication request to a further mobile device comprising at least one biometric sensor, and accomplishing biometric verification by the further mobile device and transmitting the verification result to the payment terminal.

The present invention provides the advantage that a wearable device can trigger a payment transaction including biometric verifications, wherein the wearable devices needs not to comprise a biometric sensor. Consequently, there is a technical consideration regarding the hardware efficiency of the wearable device. The wearable device can participate in a mobile payment system without the necessity to be adapted regarding the hardware requirements. Such a sensor can be provided by a further device, which holds such a sensor anyway. Accordingly, the wearable device can be coupled with a smartphone, and can use the components being provided by such a smartphone. The manufacturer needs not to install biometric sensors into the wearable device and can hence provide the wearable device at a reasonable price. Furthermore, the biometric sensor does not consume energy from the perspective of the wearable device itself. As a smartphone typically comprises a larger battery capacity compared to the wearable device computing steps can be performed by the smartphone.

There is a further technical consideration regarding the hardware capacities of the wearable device. This is the case as it is suggested to firstly evaluate a verification metric. Such a verification metric comprises rules, which indicated whether a biometric verification needs to be carried out or not. Accordingly, there may be cases, where such a verification is not necessary and therefore the respective computing steps can be omitted. This leads to further

- 5 -

hardware efficiency and a lower energy consumption of the wearable device. The verification metric is evaluated in either case meaning that even a biometric verification is not to be carried out this method step is performed. Consequently, there is a contribution over the art leading to an efficient  
5 payment procedure, which is still convenient for the user. The user convenience arises as the user is provided with a light weight and energy efficient wearable device at a reasonable price. Still, the suggested method is secure as indeed biometric verification can be performed.

- 10 A wireless payment according to the present invention is any payment, which can be triggered for instance by near field communication requiring a point-of-sale terminal. Such a point-of-sale terminal may be a wireless reading device which is provided by the point-of-sale. The user may for instance use a smartwatch as a wearable device and hold such a device against the  
15 terminal. The point-of-sale terminal thereupon registers the wearable device and transmits a transaction request.

- The transaction request may for instance comprise a specific amount of money to be paid. Furthermore, additional data may be provided by means of  
20 such a transaction request. This may comprise information regarding an ID of the point-of-sale terminal and may even provide information regarding the products to be bought.

- Of course, the point-of-sale terminal needs to verify that the user presenting  
25 the wearable device is indeed authorized to perform such transactions. Consequently, a biometric verification is suggested which lets the point-of-sale terminal identify the user. Hence, it is possible to detect, whether the wearable device is stolen and used by a thief. It may also be the case that the application scenario required that the wearable device itself needs to authenti-

- 6 -

cate the user. This may provide a security means being implemented by the manufacturer of the wearable device. Hence, in case a wearable device is stolen this device is locked for payments as the thief cannot authenticate himself before the point-of-sale terminal.

5

Consequently, it is possible to provide control instructions either on the point-of-sale terminal or the wearable device. It is also possible to use a mixed deployment providing some of the instruction on the point-of-sale terminal and further instructions on the wearable device. However, they co-  
10 operate and implement the suggested method.

Upon receiving the transaction request the provided verification metric is evaluated meaning that rules are checked which indicate, whether a biometric verification is necessary. Such a biometric verification might not be  
15 necessary in case the transaction request merely demands a small amount of money. It may furthermore be the case that only a specific number of transactions per day is possible and accordingly any further transactions are forbidden. Such considerations allow the wearable device to pay immediately or the accomplish further verification steps. In case the transaction request can  
20 be followed immediately, there is no need for performing energy consuming verification steps. Consequently, in this case the wearable device may return an acknowledgement to the point-of-sale terminal indicating that the transaction can be performed. In this way method steps are prevented which have to be performed according to known techniques.

25

In case the verification metric indicates that such authentication steps have to be performed the wearable device contacts the further mobile device and requires user authentication by means of at least one biometric sensor. For doing so, the wearable device forwards at least the authentication request to

- 7 -

the further mobile device. In this way the mobile device receives the information being necessary to identify the user. The mobile device can thereupon apply the biometric sensor for instance by means of voice recording or taking an image of the user.

5

Regarding the biometric verification it may be also advantageous to provide additional data serving as reference data. Accordingly, such reference data can be compared to actually gathered data of the user and in case both data sets are at least similar the user is authenticated. For instance, the mobile device or the wearable device stores a fingerprint of the user and upon an authentication request requests the user to provide his fingerprint over the fingerprint sensor of the mobile device. The mobile devices compares the provided fingerprint with a stored fingerprint and may then conclude that the providing user is indeed the user who is authorized to perform transactions.

15

In this way hardware and energy consuming method steps can be deployed on the mobile device again resulting in hardware efficiency of the wearable device. According to the suggested method the wearable device may use any biometric sensors being provided by a further mobile device. In case no biometric verification is required it is even not necessary to contact the mobile device and perform the required transaction immediately.

20

In case the mobile device confirms the identity of the user, the confirmation can be provided to the point-of-sale terminal, which registers that the transaction was securely paid by means of the wearable device. It may also be possible to contact further devices, such as a bank server, which performs the demanded transaction. In case the wearable device is not connected to a telecommunications network the mobile device or the point-of-sale terminal may communicate with further devices, such as a bank server. In this way the

25

- 8 -

transaction can be directly performed by the bank server and a confirmation is provided to the point-of-sale terminal. In case the biometric verification is negative, meaning that the user provides for instance a fingerprint is not the expected user a message can be provided to the wearable device or the point-  
5 of-sale terminal indicating that the procedure has terminated. It may furthermore be of advantage to provide a timeout indicating how much time a user has to perform the biometric verification. In case several attempts fail to provide the required biometric data the transaction procedure fails. It may also be of advantage to provide in addition or alternatively to the timeout a  
10 number of possible biometric verification attempts. For instance, in case the user fails to provide the required biometric data three times the authentication procedure may be terminated.

According to an aspect of the present invention the verification metric provides a set of rules indicating whether biometric verification is required re-  
15 garding the specific transaction request. This provides the advantage that for each transaction request the wearable device can decide whether to perform biometric verification. Such rules may indicate payments from a specific point-of-sale terminal always require biometric verification and on the other  
20 hand that specific point-of-sale terminals are to be paid directly without any biometric verification. Hence, the suggested method may decide from case to case whether to perform biometric verification and accordingly may save energy.

25 According to a further aspect of the present invention the verification metric considers a set of previous transaction requests. This provides the advantage that the transaction requests can be counted and upon reaching a specific number of transaction requests the transaction requests can be terminated meaning to avoid additional method steps. In this case it may be possible to

- 9 -

terminate the payment procedure in case for instance five transaction requests were already received. Furthermore, it can be restricted to process further transaction requests in case a specific number of positive transaction requests are handled. Positive transaction requests are those requests which  
5 were already paid. Hence, it is possible to define that for instance only three transaction requests can be confirmed per day. This provides an additional security means and furthermore again helps to save energy in case the transaction is terminated without any biometric verification.

10 According to a further aspect of the present invention the verification metric provides a threshold indicating a number of transactions and/or a transaction amount. This provides the advantage that the overall sum of money being spent on a day can be limited. Consequently, it may be the case that the user restricts his own wearable devices towards the payment of 500 Dollar  
15 per day. In case the wearable device is stolen the thief can only perform transactions up to the specified amount independent of further biometric verifications.

According to a further aspect of the present invention the verification metric  
20 is stored in a memory of the wearable device, the payment terminal and/or the further mobile device. This provides the advantage that the manufacturer of the respective devices or the application provider of either the point-of-sale terminal or the suggested method can implement the respective instructions on at least one of the suggested devices. Accordingly, it is possible to  
25 consider the respective application domain. This is of advantage as the transaction process is at least in part performed by the wearable device, which is administrated by the user. As critical method steps are to be performed, the service provider or the manufacturer may deploy instructions on one of the devices or several of the devices. In case the manufacturer of the point-of-sale

- 10 -

terminal implements the suggested method the critical method steps can be performed by the point-of-sale terminal. Consequently, the respective verification metric is administrated by the manufacturer himself. Consequently, there is no possibility to manipulate the verification metric, which could for instance also be stored on the wearable device. It may also be of advantage to distribute the verification metric along with respective instructions across several devices for implementing a further security means.

According to a further aspect of the present invention forwarding the verification result is performed wirelessly via the wearable device. This provides the advantage that the mobile device may use the communication interface with the wearable device, whereupon the wearable device again forwards the verification result to the point-of-sale terminal. In this case no further components are involved and the respective interface can be secured.

According to a further aspect of the present invention forwarding the verification result is performed wirelessly from the further mobile device to the payment terminal. This provides the advantage that communicating with the wearable device can be omitted and that a direct connection between the payment terminal and the mobile device can be accomplished.

According to a further aspect of the present invention forwarding the verification result is performed via a further computing device using a telecommunications network. This provides the advantage that the further computing device may be provided by a bank which directly answers the transaction request. In this case the bank server may receive the verification result along with the transaction request and may perform the requested transaction and provide the payment terminal with the respective amount of money.

- 11 -

According to a further aspect of the present invention the biometric sensor is a camera, a fingerprint sensor, a microphone or a pulse monitor. This provides that advantage that already implemented sensors of the mobile device  
5 can be used by the wearable device. Consequently, no additional hardware is required and especially no additional hardware in the wearable device itself is required. According to the biometric sensors a biometric verification can be performed without requiring additional method steps to be performed by the wearable device.

10

According to a further aspect of the present invention the wearable device is a piece of clothing, a bracelet, a watch and/or a fitness tracking device. This provides the advantage that the present invention can be implemented using commonly known wearable devices, which do not need to be updated re-  
15 garding the hardware requirements. It is rather the case that the wearable devices can be amended such that only the required instructions are to be loaded on such a wearable device. Afterwards the wearable device can participate regarding the suggested method and performing secure wireless payments may possible.

20

According to a further aspect of the present invention the further mobile device is a smartphone or a laptop computer. This provides the advantage that commonly known and typically available hardware devices are used. Hence, the user needs not to buy additional components but can rather use his  
25 commonly known wearable device and connect it to a commonly known smartphone or laptop computer. The skilled person appreciates that further hardware devices can be used, which are mobile devices.

According to a further aspect of the present invention a secure element is provided by the wearable device. This provides the advantage that specific

- 12 -

hardware features are implemented which do not allow that the stored instructions or the verification metric is manipulated. A secure element is a specific hardware device which cannot be changed by means of software as functionality is hard coded into such a secure element. Consequently, an additional security means is provided to the wearable device.

The object is also solved by a communication protocol for performing secure wireless payments using a wearable device. The communication protocol is arranged to implement the method steps as suggested by the respective method for performing secure wireless payments.

The object is also solved by a system for performing secure wireless payments using a wearable device, comprising an interface being arranged to trigger a payment transaction wirelessly by the wearable device, whereupon a transaction request and an authentication request is transmitted from a payment terminal to the wearable device, wherein a verification metric is provided indicating whether the following steps are to be performed. Namely, forwarding at least the authentication request by means of a further interface to a further mobile device comprising at least one biometric sensor. Furthermore, a biometric device is suggested being arranged to accomplish biometric verification by the further mobile device and to transmit the verification result to the payment terminal.

The suggested interfaces, namely the interface and the further interface, can be implemented as one single interface but can as well be implemented as separate interfaces allowing several ways to communicate. Such an interface may for instance be formed by Bluetooth, near field communication or in general by a telecommunications network.

- 13 -

The skilled person appreciates that further hardware components can be provided which are required for implementing the suggested system. Such further components may for instance comprise network components such as a router or a server.

5

The object is also solved by a computer program product being arranged to perform the suggested method or operated the suggested system. A computer program product may also store the suggested protocol.

- 10 The skilled person appreciates that the method provides method steps which can be implemented as structural features as well. Accordingly, the suggested system provides structural features which can be implemented in accordance with their method steps and the method steps provide functionality which can as well be implemented in hardware of the suggested system. The
- 15 computer program product performs the suggested method steps and at least in part operates the system for performing secure wireless payments using the wearable device.

20 The invention is now described with reference to the accompanying figures, which show:

- Fig. 1: a schematic flow chart illustrating a method for performing secure wireless payments according to an aspect of the present invention; and
- 25 Fig. 2: a system arrangement for performing secure wireless payments according to a further aspect of the present invention.

Fig. 1 shows a method for performing secure wireless payments using a wearable device, comprising the steps of triggering 100 a payment transac-

- 14 -

tion wirelessly by the wearable device, whereupon a transaction request and an authentication request is transmitted 101 from a payment terminal to the wearable device, wherein a verification metric is provided indicating 102 whether the following steps are to be performed. Namely, forwarding 103 at  
5 least the authentication request to a further mobile device comprising at least one biometric sensor and accomplishing 104 biometric verification by the further mobile device and transmitting the verification result to the payment terminal. In step 102 it is decided whether biometric verification needs to be accomplished and in case this has not to be performed the method performs  
10 the required transaction. Furthermore, in case the biometric verification being accomplished in step 104 is negative, the suggested method terminates. In this case no transaction request is confirmed.

The skilled person appreciates the aforementioned method steps can be per-  
15 formed iteratively and/or in a different order. It may also be the case that further substeps are required.

Fig. 2 shows a system for performing secure wireless payments using a wearable device. In Fig. 2 on the left top there is depicted a point-of-sale terminal at which a customer wants to perform a payment transaction using his  
20 wearable device. The wearable device is shown on the left hand side at the bottom of Fig. 2. The wearable device communicates with a companion device comprising a biometric sensor. This device is shown on the right hand side, bottom of Fig. 2. On the top right hand side of Fig. 2 a bank host system  
25 is depicted. According to the suggested system risk management can be enhanced by allowing the payment application on a wearable device to request biometric verification data of the card holder on a companion device like smartphone or tablet computer. The biometric input, for instance a fingerprint, an iris scan, a facial scan or any other supported biometric sample, is

- 15 -

required after a number of transactions and/or accumulated spend or in the case of the transaction amount exceeds a predefined threshold. Provided that the biometric sample is a match with a verification value previously stored in the wearable device, the risk management counters could be reset.

5

The suggested method and system can be summarized as follows. While using a wearable for payment purposes and the wearable does not have an interface for biometric input, risk management can be enhanced by allowing the payment application on a wearable device to request biometric verification data of the cardholder on a companion device like smartphone or tablet. A payment application, or alternatively a separate application which carries out biometric data verification on behalf of the payment application, in a Secure Element on a wearable device could ask for biometric input after a number of transactions and/or accumulated spend, or in the case of the transaction amount exceeds a pre-defined threshold. The status of the application could be displayed to the device holder in an application on a companion device. The user could then start a session e. g. from a secure wallet application on the companion device, which would further start a Bluetooth-connection to the wearable device. User would then be requested to provide a biometric sample (e. g. finger print, iris scan, facial scan or any other supported biometric sample) on the companion device, which would process the sample into a format suitable for verification in the applications in the wearable device. Provided the biometric sample is a match with a verification value previously stored in the wearable device, the risk management counters could be reset.

10

15

20

25

In case the biometric would be used as user verification for large ticket items, the wearable could ask for biometric verification for a payment transaction when a pre-defined amount is exceeded. In this case the application on the

- 16 -

wearable would request the user to provide a biometric sample for further processing and in case of a positive match, payment can be authorized and processed.

- 5     There is no need to integrate a biometric reader in the wearable device itself, which allows for lower cost of materials for the device. Whilst the wearable is affordable it still allows for highly secure transaction for end users and lower risks for issuing organizations. The combination of a wearable and a companion device for the objective of strong user verification makes use of exist-
- 10    ing infrastructure in many mobile phones and tablets already capable to perform biometric data capture and processing.

- Summarizing the above method, a protocol and a system along with a respectively arranged computer program product is suggested allowing the
- 15    wearable device to decide whether to perform biometric verification and thereupon save energy and hardware capacities in case biometric verification is not required.

### Claims

- 5     1.     A method for performing secure wireless payments using a wearable device, comprising the steps:
- 10           -     triggering (100) a payment transaction wirelessly by the wearable device, whereupon a transaction request and an authentication request is transmitted (101) from a payment terminal to the wearable device, characterized in that a verification metric is provided indicating (102) whether the following steps are to be performed:
- 15           -     forwarding (103) at least the authentication request to a further mobile device comprising at least one biometric sensor; and
- accomplishing (104) biometric verification by the further mobile device and transmitting the verification result to the payment terminal.
- 20     2.     The method according to claim 1, characterized in that the verification metric provides a set of rules indicating whether biometric verification is required regarding the specific transaction request.
- 25     3.     The method according to claim 1 or 2, characterized in that the verification metric considers a set of previous transaction requests.
4.     The method according to any one of the preceding claims, characterized in that the verification metric provides a threshold indicating a number of transactions and/or a transaction amount.

- 18 -

5. The method according to any one of the preceding claims, characterized in that the verification metric is stored in a memory of the wearable device, the payment terminal and/or the further mobile device.  
5
6. The method according to any one of the preceding claims, characterized in that forwarding (103) the verification result is performed wirelessly via the wearable device.
- 10 7. The method according to any one of the preceding claims 1 to 5, characterized in that forwarding (103) the verification result is performed wirelessly from the further mobile device to the payment terminal.
8. The method according to any one of the preceding claims 1 to 5, characterized in that forwarding (103) the verification result is performed via a  
15 further computing device using a telecommunications network.
9. The method according to any one of the preceding claims, characterized in that the biometric sensor is a camera, a fingerprint sensor, a microphone or a pulse monitor.  
20
10. The method according to any one of the preceding claims, characterized in that the wearable device is a piece of clothing, a bracelet, a watch and/or a fitness tracking device.  
25
11. The method according to any one of the preceding claims, characterized in that the further mobile device is a smartphone or a laptop computer.

- 19 -

12. The method according to any one of the preceding claims, characterized in that a secure element is provided by the wearable device.
13. A communication protocol for performing secure wireless payments  
5 using a wearable device, comprising:
- triggering (100) a payment transaction wirelessly by the wearable device, whereupon a transaction request and an authentication request is transmitted (101) from a payment terminal to the wearable device, characterized in that a verification metric is provided indicating (102)  
10 whether the following steps are to be performed:
  - forwarding (103) at least the authentication request to a further mobile device comprising at least one biometric sensor; and  
15
  - accomplishing (104) biometric verification by the further mobile device and transmitting the verification result to the payment terminal.
14. A system for performing secure wireless payments using a wearable  
20 device, comprising:
- an interface being arranged to trigger (100) a payment transaction wirelessly by the wearable device, whereupon a transaction request and an authentication request is transmitted (101) from a payment terminal to  
25 the wearable device, characterized in that a verification metric is provided indicating (102) whether the following structural features are addressed:

- 20 -

- a further interface being arranged to forward (103) at least the authentication request to a further mobile device comprising at least one biometric sensor; and
- 5    - a biometric device being arranged to accomplish (104) biometric verification by the further mobile device and to transmit the verification result to the payment terminal.
- 15.   A computer program product being arranged to perform a method in  
10    accordance with any one of the preceding claims 1 to 12.

1/2

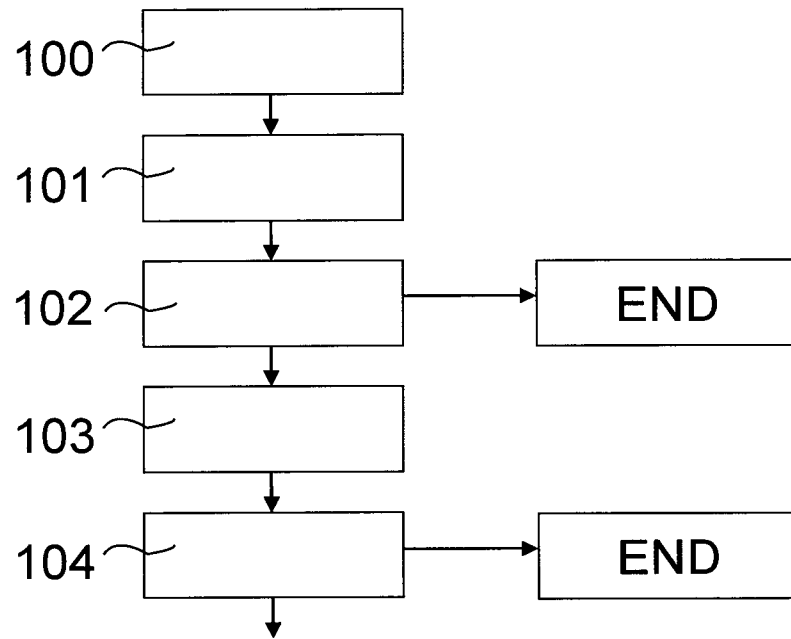


Fig. 1

2/2

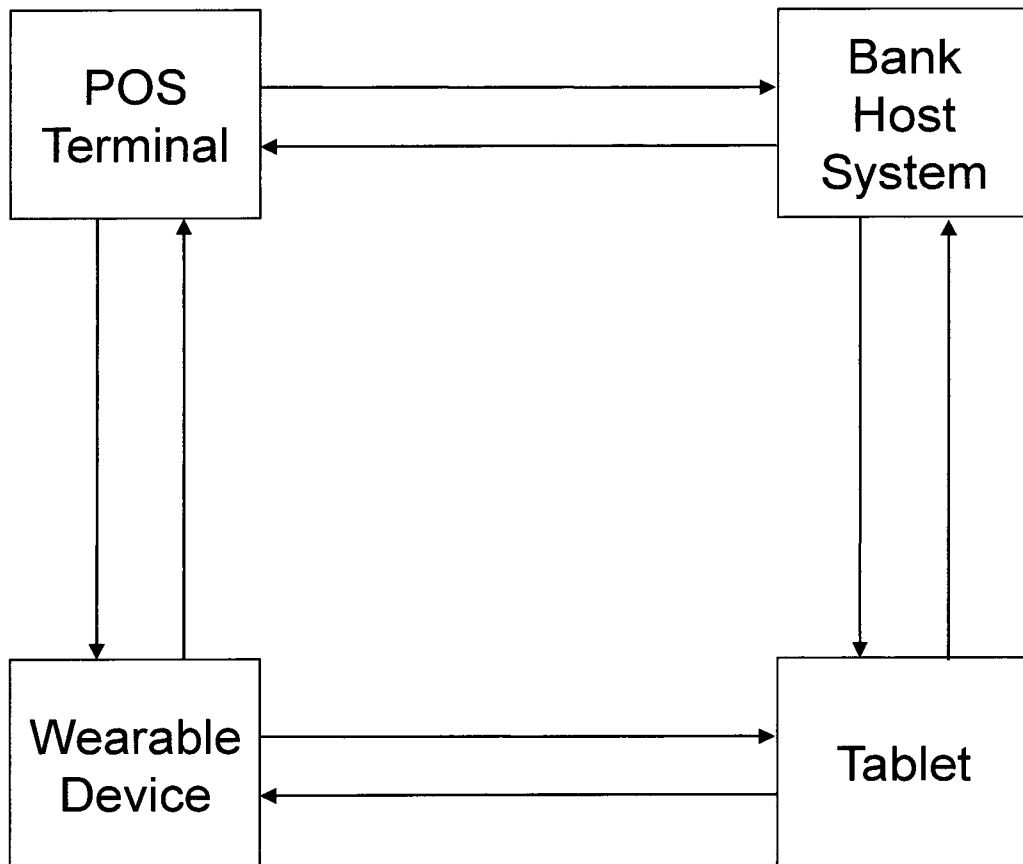


Fig. 2

## INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2017/000921

## A. CLASSIFICATION OF SUBJECT MATTER

INV. G06Q20/30 G06Q20/32 G06Q20/40  
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 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 2014/282878 A1 (IGNATCHENKO SERGEY [AT] ET AL) 18 September 2014 (2014-09-18)<br>figures 1,3a,6<br>paragraph [0020] - paragraph [0035]<br>paragraph [0056] - paragraph [0057]<br>paragraph [0030] | 1-15                                  |
| X         | US 2016/086186 A1 (CANDELORE BRANT [US] ET AL) 24 March 2016 (2016-03-24)                                                                                                                            | 1-5,8,9,<br>11,12,<br>14,15<br>6,7,10 |
| A         | figures 1-3,5-6,8,10-11,14-15<br>paragraph [0043] - paragraph [0096]<br>paragraph [0104] - paragraph [0105]<br>-----<br>-/-                                                                          |                                       |



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 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

"&amp;" document member of the same patent family

Date of the actual completion of the international search

14 August 2017

Date of mailing of the international search report

22/08/2017

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

Raymaekers, Jens

## INTERNATIONAL SEARCH REPORT

International application No  
PCT/EP2017/000921

| C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT |                                                                                                                                                                                                                     |                       |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Category*                                            | Citation of document, with indication, where appropriate, of the relevant passages                                                                                                                                  | Relevant to claim No. |
| A                                                    | WO 2016/109087 A1 (PAYPAL INC [US])<br>7 July 2016 (2016-07-07)<br>figures 1-5<br>paragraph [0003]<br>paragraph [0015] - paragraph [0030]<br>paragraph [0042] - paragraph [0043]<br>-----                           | 1-15                  |
| A                                                    | US 7 637 434 B2 (BEENAU BLAYN W [US] ET<br>AL) 29 December 2009 (2009-12-29)<br>figure 9<br>page 7, line 30 - page 7, line 38<br>page 11, line 59 - page 12, line 3<br>page 28, line 38 - page 29, line 17<br>----- | 1-15                  |
| A                                                    | US 7 597 265 B2 (BONALLE DAVID S [US] ET<br>AL) 6 October 2009 (2009-10-06)<br>page 64, line 42 - page 65, line 26<br>-----                                                                                         | 1-15                  |
| A                                                    | US 2016/099938 A1 (SEO YOUNG-JUN [KR] ET<br>AL) 7 April 2016 (2016-04-07)<br>figures 1-3<br>paragraph [0090]<br>paragraph [0008]<br>-----                                                                           | 1-15                  |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2017/000921

| Patent document<br>cited in search report | Publication<br>date | Patent family<br>member(s)  | Publication<br>date         |
|-------------------------------------------|---------------------|-----------------------------|-----------------------------|
| US 2014282878                             | A1                  | 18-09-2014                  | CA 2902290 A1 18-09-2014    |
|                                           |                     | EP 2973275 A1 20-01-2016    |                             |
|                                           |                     | TW 201443798 A 16-11-2014   |                             |
|                                           |                     | US 2014282878 A1 18-09-2014 |                             |
|                                           |                     | WO 2014141158 A1 18-09-2014 |                             |
| -----                                     |                     |                             |                             |
| US 2016086186                             | A1                  | 24-03-2016                  | CN 105447694 A 30-03-2016   |
|                                           |                     | JP 6143021 B2 07-06-2017    |                             |
|                                           |                     | JP 2016071878 A 09-05-2016  |                             |
|                                           |                     | KR 20160035547 A 31-03-2016 |                             |
|                                           |                     | US 2016086186 A1 24-03-2016 |                             |
|                                           |                     | US 2017039545 A1 09-02-2017 |                             |
| -----                                     |                     |                             |                             |
| WO 2016109087                             | A1                  | 07-07-2016                  | US 2016189136 A1 30-06-2016 |
|                                           |                     | WO 2016109087 A1 07-07-2016 |                             |
| -----                                     |                     |                             |                             |
| US 7637434                                | B2                  | 29-12-2009                  | US 2004230488 A1 18-11-2004 |
|                                           |                     | US 2007296544 A1 27-12-2007 |                             |
|                                           |                     | US 2008010161 A1 10-01-2008 |                             |
|                                           |                     | US 2008015941 A1 17-01-2008 |                             |
|                                           |                     | US 2008016002 A1 17-01-2008 |                             |
|                                           |                     | US 2009119220 A1 07-05-2009 |                             |
|                                           |                     | US 2009125401 A1 14-05-2009 |                             |
|                                           |                     | US 2009171851 A1 02-07-2009 |                             |
|                                           |                     | US 2017228738 A1 10-08-2017 |                             |
| -----                                     |                     |                             |                             |
| US 7597265                                | B2                  | 06-10-2009                  | US 2006016877 A1 26-01-2006 |
|                                           |                     | US 2008015994 A1 17-01-2008 |                             |
|                                           |                     | US 2008173708 A1 24-07-2008 |                             |
|                                           |                     | US 2009289112 A1 26-11-2009 |                             |
|                                           |                     | US 2010312698 A1 09-12-2010 |                             |
|                                           |                     | US 2011288993 A1 24-11-2011 |                             |
|                                           |                     | US 2014081857 A1 20-03-2014 |                             |
| -----                                     |                     |                             |                             |
| US 2016099938                             | A1                  | 07-04-2016                  | KR 20160040872 A 15-04-2016 |
|                                           |                     | US 2016099938 A1 07-04-2016 |                             |
| -----                                     |                     |                             |                             |