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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 April 2019 (18.04.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/074686 A1

(51) International Patent Classification:
G06Q 20/00 (2012.01)

(21) International Application Number:
PCT/US2018/053293

(22) International Filing Date:
28 September 2018 (28.09.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
17195532.1 09 October 2017 (09.10.2017) EP

(71) Applicant: **MASTERCARD INTERNATIONAL INCORPORATED** [US/US]; 2000 Purchase Street, Purchase, NY 10577 (US).

(72) Inventors: **BLINOV, Mikhail**; 5 Ashgrove, Dun Laoghaire, Dublin (IE). **NOWAK, Dawid**; 3 Blackwood Mews, Ongar Chase, Dublin 15 (IE). **DRUTA, Vladut**; 41 Dorset Square, Upper Gardiner Street, Dublin 1 (IE). **BURNS, Cian**; 61 Clonea, Ballinteer, Dublin 16 (IE). **CUNNION, Aidan**; 16 Wainsfort Road, Terenure, Dublin 6W (IE).

(74) Agent: **DOBBYN, Colm, J.**; Mastercard International Incorporated, 2000 Purchase Street, Purchase, NY 10577 (US).

(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,

(54) Title: A SYSTEM AND METHOD FOR PERFORMING PEER TO PEER TRANSFERS

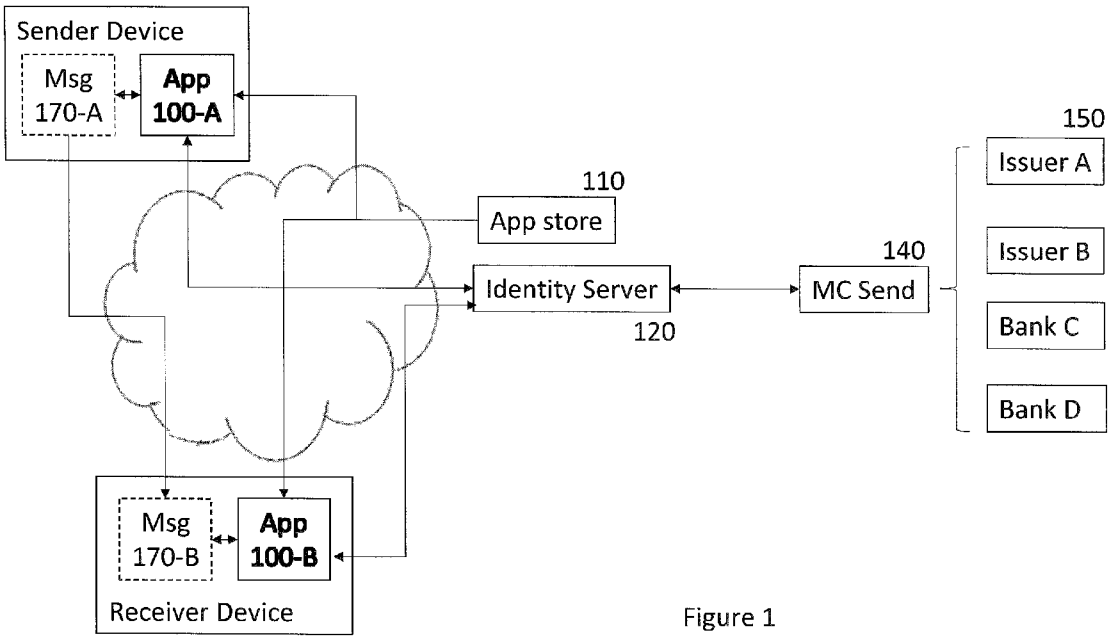

Figure 1

(57) Abstract: In a first party mode, a peer-to-peer transfer application: authenticates the party to an identity server; obtains an amount of funds to be transferred; causes the identity server to establish a session for storing information relating to the transaction; provides the amount to the identity server; provides account information for the party to the identity server; obtains a token unique to the transaction; obtains contact information for the counterparty: and provides a message including the token to the counterparty to indicate that the transaction has been initiated. In a second counterparty mode, the application: receives a message from a first party, the message including a token for a transaction; authenticates the counterparty; determines that the counterparty wishes to complete the transaction; and uses the token to provide account information for the counterparty to the identity server for storing in association with an established session for the transaction and to enable the identity server to complete the transaction.

WO 2019/074686 A1

[Continued on next page]

MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

A SYSTEM AND METHOD FOR PERFORMING PEER TO PEER TRANSFERS

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit of, and priority to, European Patent Application No. 17195532.1 filed on October 9, 2017. The entire disclosure of the above application is incorporated herein by reference.

FIELD

The present invention relates to a system and method for performing peer to peer transfers.

BACKGROUND

Payment applications which can be installed on end user devices such as smartphones, tablets or even general purpose computers to enable peer-to-peer payments between a payer and payee, generally require that the details of the payee are provided when payment is initiated by a payer. This implies that every payer either needs to obtain, input and store the bank account details for any payee to which they wish to make a payment; or rely on a common system to provide those.

For the former in particular, the burden of having a payer receive account details, which can involve relatively long numbers, potentially from many different payees, has acted as one barrier to adoption of such payment applications. Thus, unsurprisingly the market for peer-to-peer payments has not taken off yet and there are many applications such as from Skype or Paypal with relatively low market penetration or usage.

SUMMARY

According to the present invention, there is provided a method for performing a peer to peer transfer according to claim 1.

In a second aspect there is provided a computer program product comprising a computer readable medium on which instructions are stored which, when executed on a computer system, is configured for performing a method for performing a peer to peer transfer according to claim 1.

In a third aspect there is provided a device for performing a peer-to-peer transfer according to claim 1.

Embodiments of the invention combine ease of use and adoption with a high degree of trust and security for users.

Embodiments allow for the transfer of funds between peers without necessarily having to create an account or log into an account. Participating parties (sender and receiver) can be correlated through an ephemeral session key which changes from transaction to transaction.

Embodiments can be based on biometric authentication so avoiding the need for a user to generate or remember new usernames or passwords.

Embodiments are based on a two phase payment strategy. This means that a one party's payment credentials don't need to be known or disclosed to the counter-party when a payment is initiated. An additional benefit of such a system is that payment details do not have to be stored centrally.

The end user application can either be implemented as a stand-alone funds transfer application or the functionality can be embedded within other applications such as e-commerce or M-commerce applications, for example, to facilitate electronic payments not alone from customer to customer, but also from customer to merchant or merchant to merchant, thus payments can be facilitated between many different operators.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a diagram illustrating the interoperating components of a payment system according to an embodiment of the present invention;

Figure 2 illustrates the steps performed by an application operated by a payer (sender) in communication with an identity server from Figure 1;

Figure 3 illustrates the steps performed by the identity server in communication with an application operated by a payee (receiver) from Figure 1; and

Figure 4 illustrates the steps performed by the identity server in communication with a payment gateway from Figure 1.

DESCRIPTION OF THE EMBODIMENTS

Referring now to Figure 1, in a payment system according to an embodiment of the present invention, a user of a device through which they wish to initiate a payment first installs a payment application on their device.

As will be appreciated, where the device is a typical smartphone or tablet based on the Android or iOS operating systems, the user can download such an application from an app store 110. Alternatively, especially where the device is a Windows based desktop or laptop device, but this can also be the case for a smartphone, the user can download the application from an application provider website. In a still further variation, rather than a stand-alone client application, the application can be implemented as a browser based application.

In any case, the initiating user can either be a payer (sender) or a payee (receiver) and the example below will be described with reference to a payment being initiated by a sender.

Referring now to Figure 2, when the sender first executes their application 100-A, on their device, they register their identity with an identity server 120. In one implementation, they do so based on FIDO ("Fast IDentity Online") protocols defined by the FIDO Alliance. FIDO protocols use standard public key cryptography techniques to provide authentication. During registration with the identity server 120, the user's application 100-A creates a new key pair. The application 100-A retains the private key and registers the public key with the online server 120. Subsequent authentication is done by the user through the application 100-A proving possession of the private key to the server by signing a challenge. The client's private keys can be used only after they are unlocked locally on the device by the user. The local unlock is accomplished by a user–friendly and secure action such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second–factor device or pressing a button or indeed using any form or combination of biometric information.

The FIDO protocols are designed to protect user privacy as they do not provide information that can be used by different online services to collaborate and track a user across the services. Biometric information, if used, never leaves the user's device.

Accordingly, at step [001], the sender's application 100-A connects with the identity server 120 and requests a challenge by way of registration request

which is provided by the identity server at step [002]. On receipt of the challenge, from the identity server 120, the sender's application 100-A captures the required user's biometrics, step [003]. As indicated, this can comprise any combination of swiping a finger, entering a PIN, speaking into a microphone, inserting a second–factor device or pressing a button etc. A response including a public key for the sender based on the user's biometrics is provided back to the identity server 120 at step [0004] and once the public key is registered, this is confirmed by the identity server 120 to the sender application 100-A at step [005].

The sender can now decide to send money using their instance of the application 100-A at any subsequent time. (Indeed as will be explained later, once they have installed their instance of the application 100-A and registered with the identity server 120, they are also in a position to receive requests from potential payees.)

In the example, of Figure 2, the sender application 100-A is installed on a mobile (cellular) device with a phone number as an identifier and so a secure channel based on the phone number can be established between the sender application 100-A and the identity server 120 based on that identifier, step [007]. It will be appreciated that in other embodiments where the sender application 100-A is installed on a non-mobile device, an equivalent secure channel can be established using other mechanisms or based on other identifiers for example a MAC identifier. In any case, in response to establishing the channel, a session can be established, step [008] and acknowledged by the identity server 120 to the sender application 100-A, step [009]. As will be seen, the session established within the identity server 120 acts as a placeholder for the information required for any given transaction.

In the embodiment, once the sender application 100-A receives notification of establishment of the session, the application 100-A can prompt the sender for a message associated with the payment, step [010]. In the example, at step [011], the user enters the free form message "hey, here is the 20USD that I owe you". At steps [012] and [013], the user actually enters a monetary amount to be transferred. It will of course be appreciated that any suitable mechanism can be employed to enable the user to determine the amount of the payment to be made and any message to accompany the payment.

At steps [014] and [015], the identity server 120 requests and the sender application 100-A provides the sender's bank account details from which the funds will be transferred.

Thus, if the user has not already stored bank account details in the application, they will be prompted to do so, and if they have provided details of more than one account to the application 100-A, they will be prompted to select an account before these details are returned to the identity server 120.

The user can now authenticate themselves to the identity server 120, through steps [016] to [021]. As will be seen, the information required to be provided by the user for authentication can be based on any combination of the device they are employing, the user's profile and the amount of the transfer as determined by an authentication rules engine 130 operating in conjunction with the identity server 120. Such policy based authentication is disclosed, for example, in European Publication No. EP2605567 in the name of Daon Holdings Limited and related applications.

Once the sender is authenticated, the sender application 100-A sends the data gathered at steps [010] to [015] to the identity server 120, step [022]. In this regard, it will be seen that any of steps [010] to [015] could also follow authentication steps [016] to [021].

The identity server 120 now updates information for the session created at step [008] with the transaction data received from the sender application 100-A at step [023] and generates a unique token for the transfer at step [024]. Thus, the token acts as an ephemeral key to the session for the transaction. The token is provided to the sender application 100-A at step [025] and the sender application 100-A can now use the token to generate a message to be provided to the receiver in order to complete the transaction.

In one embodiment, the application 100-A has access to a contact list installed on the device and which the user normally uses to generate SMS or instant messenger (IM) messages, initiate calls and/or generate e-mails or indeed to facilitate any interaction with their various social networks.

Thus, on receipt of the token from the identity server 120, the application 100-A can request that the sender select a contact from the contact list, step [027] in order to determine the type of message which needs to be generated for the receiver. So where a sender's phone number is selected from a contact list, the application can generate an SMS or IM message including the message and amount

entered at steps [011] and [013] as well as a URL generated at step [026] from the token provided by the identity server. The URL enables a receiver of the message to automatically launch an instance of the application on a separate device with the application then displaying the payment message and other details for the transaction identified by the token.

If the sender selects a receiver e-mail address from their contact list, the message generated at step [028] would comprise an e-mail message. This allows fuller information to be included in the message including information relating to the payment application and for example links enabling a user who has not installed the payment application on their device to do so.

In any case, once the message has been generated at step [028], the sender application can send the message using the appropriate API exposed by the sender device corresponding messaging or e-mail application 170-A, step [029].

Note that in the example of Figure 2, registration and authentication are performed separately. However, it will be appreciated that when a user first registers with the identity server 120 and then immediately wishes to initiate a payment (either as a payer or payee), steps [016] to [021] may not need to be performed.

Referring now to Figure 3, which shows the steps performed by a receiver who has not previously installed a payment application on their device.

Step [030] shows the receipt of the message sent by the payer and as will be appreciated, this could appear in any of a messaging application, IM application or e-mail inbox 170-B a receiver has installed on their device.

If the user has not installed the application on their device, the message can enable them to do so by including direct links to the application on the app store 110 or any repository for the application software.

Once the application 100-B is installed, it can be launched from the message at step [031], for example, by clicking on the URL within the message generated at step [026].

If the user has not previously installed and registered themselves with the application 100-B, they do so in steps [034] to [038] as in the case of the sender in steps [001] to [005].

Once again, a secure channel is established between the receiver application 100-B and the identity server, steps [032] and [033] and it will be seen

that these steps can be performed either before or after steps [034] to [038], although it is preferred that FIDO registration be performed on a secure channel.

The original token from the message received at step [030] can now be used by the application 100-B to indicate to the identity server 120 the session to which the transaction relates and to retrieve the payment data from the session data stored by the identity server 120, steps [039] to [041].

The application 100-B can now display the sender's detail, description and amount for the payment, step [042], enabling the receiver to accept (or reject) the payment.

If the receiver accepts the payment and they have not authenticated themselves to the receiver application 100-B, they can now do so in steps [045] to [050], again using the authentication rules engine 130 to determine the biometric information to be provided by the receiver.

Again, in the example of Figure 3, registration and authentication are performed separately. However, it will be appreciated that when a user first registers with the identity server 120 and then immediately wishes to complete a payment (either as a payer or payee), steps [045] to [050] may not need to be performed.

Again, at steps [051] and [052], the identity server 120 requests and the receiver application 100-B provides the receiver's bank account details from which the funds will be transferred.

Thus, if the receiver has not already stored bank account details in the application 100-B, they will be prompted to do so, and if they have provided details of more than one account to the application 100-B, they will be prompted to select an account before these details are returned to the identity server 120, at step [053], along with the token provided in the original message received at step [030].

This enables the identity server 120 to add the receiver details to the session data originally established by the sender, step [054], and to collate this data, step [055].

Turning now to Figure 4, once the data for a payment is correlated and complete, the identity server 120 can now provide the information to a payment gateway. An exemplary gateway is provided by Mastercard and is referred to as MC Send 140 and this gateway exposes an API enabling a variety of other forms of application to provide transaction details including sender and receiver account details and transaction amount to be executed by the gateway.

Using such a gateway enables a variety of types of transaction to be completed and so for example either of the sender or receiver can specify credit card, debit card or bank account details and a payment gateway such as provided by Mastercard can complete a transfer of the funds accordingly by initiating appropriate messages to the issuers 150 for the credit or debit cards or the banks corresponding to the account information specified by the sender and or receiver.

Before doing so, the payment gateway 140 may check the transaction with a fraud rules engine (gatekeeper) 160 of the type provided by Mastercard or Kount. Gatekeeper servers are typically used to prevent credit card fraud by enabling a merchant to check whether or not a card is valid. They essentially comprise a rules based engine for identifying fraudulent or potentially invalid payment card use and/or databases which can store lists of lost, blocked or stolen payment cards. These rules can include rules for analysing whether a payment card of a particular type, even though valid, can be accepted by a given merchant.

In any case, if the check is in order, the payment gateway 140 can finalise the payment, step [058]. Once complete the payment gateway 140 notifies the identity server 120 at step [059] as to whether or not the payment was completed and this information is notified in turn to each of the sender and receiver application, step [060] and these notify the sender and receiver at steps [061] and [062] respectively. The session established at step [008] can now be terminated by the identity server 120, step [063].

As indicated above, it will be appreciated that the implementations of the application 100 can be extended to enable a potential receiver of funds to initiate a transfer. In this case, once authenticated to the identity server 120 at a device the potential receiver can specify a message and an amount (as in steps [010] to [014]) as well as select a potential sender (as in step [027]) so that the application can generate a message to be sent to the potential sender (as in step [029]). In this case, it is the receiver application which establishes a session within the identity server 120 and which initially generates and provides the data for the session with the instance of sender application subsequently providing their data to complete the information required for the session and to enable the transfer to be executed.

It will be appreciated that many variants of the above embodiment are possible. For example, rather than generating a message to be sent to a contact using a messaging service external to the payment application, as in steps [028] and [029], the

payment application could instead provide an identifier for the counter-party, i.e. either the sender or receiver, directly to the identity server 120, for example, their phone number, e-mail address or username/nickname or other form of identity, for example, a Google handle.

On receipt of such a message, the identity server 120, could determine if the counterparty is registered i.e. that they had installed the application and registered with the application. In this case, identity server 120 could send a push notification including the token directly to the counter-party device, so enabling the counter-party device to execute steps [032], [033] and [039] to [042] automatically.

In another variation, a sender could provide additional information for or about a potential receiver of funds, so that the identity server 120 might more securely establish the receiver's credentials. Thus, before completing a transaction a sender and receiver might communicate with one another out-of-band in order to establish a private transaction specific codeword sent by the transaction initiator along with the other payment details.

Alternatively, rather than using agreed upon additional information, the initiating party could specify additional authentication information they expect the counterparty to possess.

In other variations, a sender could request a stronger or weaker authentication policy for a receiver. Alternatively or in addition, a sender could request that authentication has to be done on a specific device, for example by providing phone number. In this case, the application would check that the number on which the receiver establishes their secure session matches the specified number before proceeding with the transaction.

In other variations, instances of the application 100 and identity server 120 could operate in conjunction with an online wallet, with the participant providing access details to their online wallet from where identity server 120 could retrieve the payment details of either a sender or receiver account.

It will be appreciated that the application operated by each party to a transaction could be an instance of the same application or the functionality described above for the application could be integrated within a multi-function platform such as an e-commerce or m-commerce application so that in some cases, one party may operate a different application than another to complete a given transaction.

Note that FIDO registration/authentication can also be executed through a browser rather than through a stand-alone application 100 such as described above. As such, it is possible for certain parties, for example, merchants, to operate within the system through a browser based application rather than a dedicated application.

CLAIMS:

1. A method performed by an application installed on a computing device operated by a party to a transaction for performing a peer-to-peer transfers, the method comprising the application:

in a first party mode:

authenticating the party to an identity server;

obtaining from the party an amount of funds to be transferred between said party and a counterparty;

causing said identity server to establish a session for storing information relating to said transaction;

providing said amount to said identity server for storing in association with said session;

providing account information for said party to said identity server for storing in association with said session;

obtaining a token unique to said transaction from said identity server;

obtaining contact information for the counterparty; and

providing a message including said token to said counterparty using said contact information to indicate to said counterparty that said transaction has been initiated; and

in a second counterparty mode:

receiving a message from a first party to a transaction, the message including a token for a transaction;

authenticating the counterparty to the identity server;

determining that said counterparty wishes to complete said transaction; and

responsive to said determining, using said token to provide account information for said counterparty to said identity server for storing in association with an established session for said transaction and to enable said identity server to complete said transaction; and

receiving results for any completed transaction from said identity server.

2. A method according to claim 1 wherein:

said providing a message comprises said application sending said message using an application programming interface, API, for a messaging application installed on said computing device; and

said receiving a message comprises said application receiving said message through being launched using an application programming interface, API, for said application from a messaging application installed on said computing device.

3. A method according to claim 1 wherein:

said providing a message comprises said application sending said message through said identity server; and

said receiving a message comprises said application receiving said message from said identity server.

4. A method according to claim 1 wherein said authenticating is performed based on a FIDO, Fast IDentity Online, protocol.

5. A method according to claim 1 wherein said first party is one of a payer or a payee and said counterparty is the other of said payer and said payee.

6. A method according to claim 1 wherein in said first party mode, said application is arranged to specify authentication criteria for said counterparty to said transaction.

7. A method according to claim 1 wherein said application is integrated within an application providing functionality other than funds transfer.

8. A method according to claim 1 wherein said application is cooperable with an electronic wallet to retrieve said account information for said party and/or counterparty.

9. A method according to claim 1 wherein said message comprises instructions for a counterparty to enable a counterparty to install said application on their device.

10. A method according to claim 2 wherein said messaging application comprises any one of an SMS application; and instant messenger application; or an e-mail application.

11. A method according to claim 1 wherein said obtaining contact information comprises said application obtaining contact information from a contact list for said first party and displaying said contact list for selection of a counterparty contact.

12. A computer program product comprising a computer readable medium on which instructions are stored which, when executed on a computing device, is configured for performing the steps of claim 1.

13. A computer program product according to claim 1 comprising instructions executable either as a stand-alone client application; or as a browser based application.

14. A computing device for performing a peer-to-peer transfer and including an application arranged to perform the method of claim 1.

150
Issuer A
Issuer B
Bank C
Bank D
140
MC Send
110
App store
Identity Server
120
Sender Device
App
100-A
Msg
170-A
App
100-B
Msg
170-B
Receiver Device

Figure 1

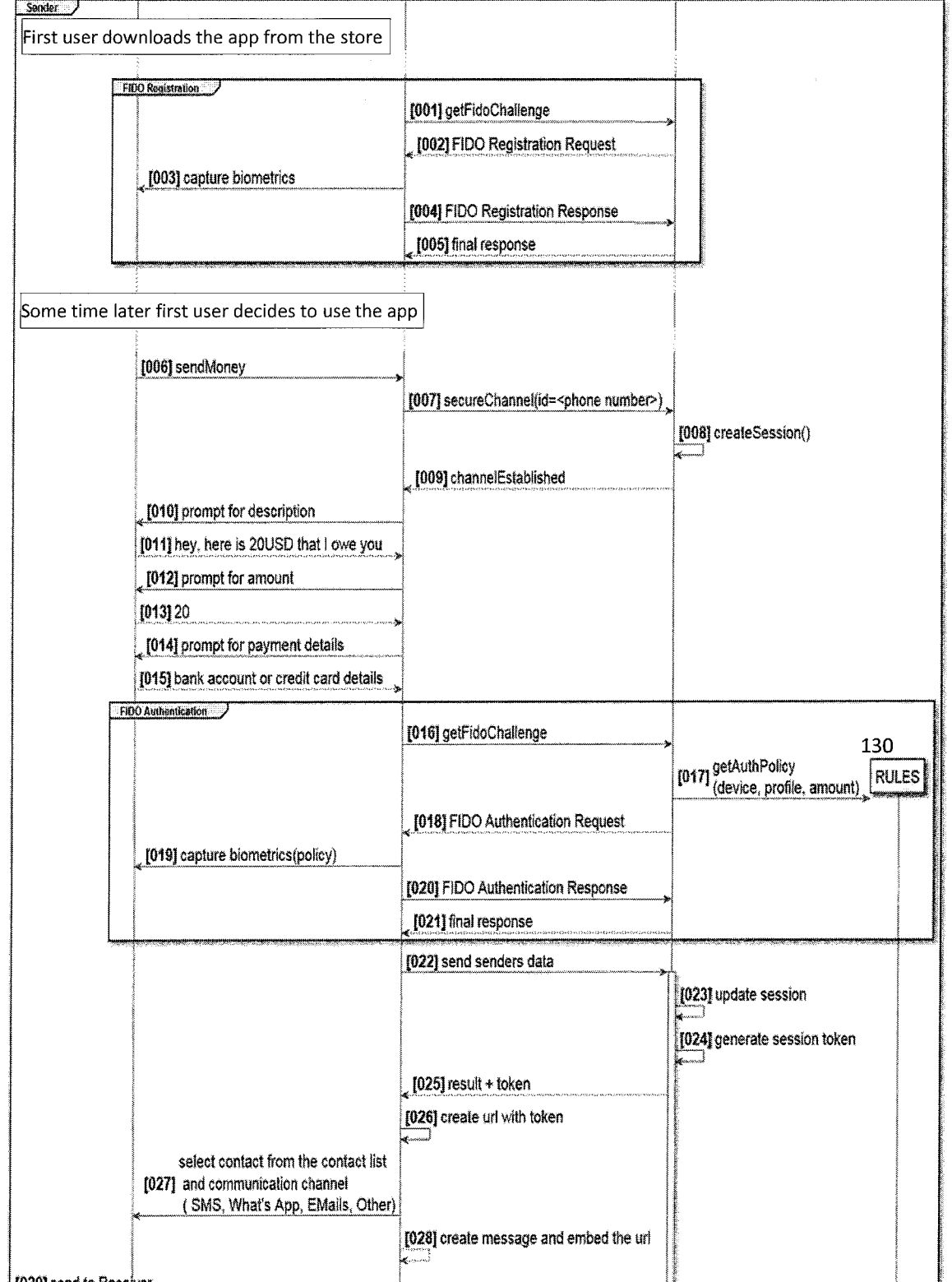
100-A
Sender
Sender's App
MIS
Sender
First user downloads the app from the store
FIDO Registration
[001] getFidoChallenge
[002] FIDO Registration Request
[003] capture biometrics
[004] FIDO Registration Response
[005] final response
Some time later first user decides to use the app
[006] sendMoney
[007] secureChannel(id=<phone number>)
[008] createSession()
[009] channelEstablished
[010] prompt for description
[011] hey, here is 20USD that I owe you
[012] prompt for amount
[013] 20
[014] prompt for payment details
[015] bank account or credit card details
FIDO Authentication
[016] getFidoChallenge
130
[017] getAuthPolicy
(device, profile, amount)
RULES
[018] FIDO Authentication Request
[019] capture biometrics(policy)
[020] FIDO Authentication Response
[021] final response
[022] send senders data
[023] update session
[024] generate session token
[025] result + token
[026] create url with token
select contact from the contact list
[027] and communication channel
(SMS, What's App, EMails, Other)
[028] create message and embed the url
[029] send to Receiver
170-A
Sender
Sender's App
MIS
120
RULES

Figure 2

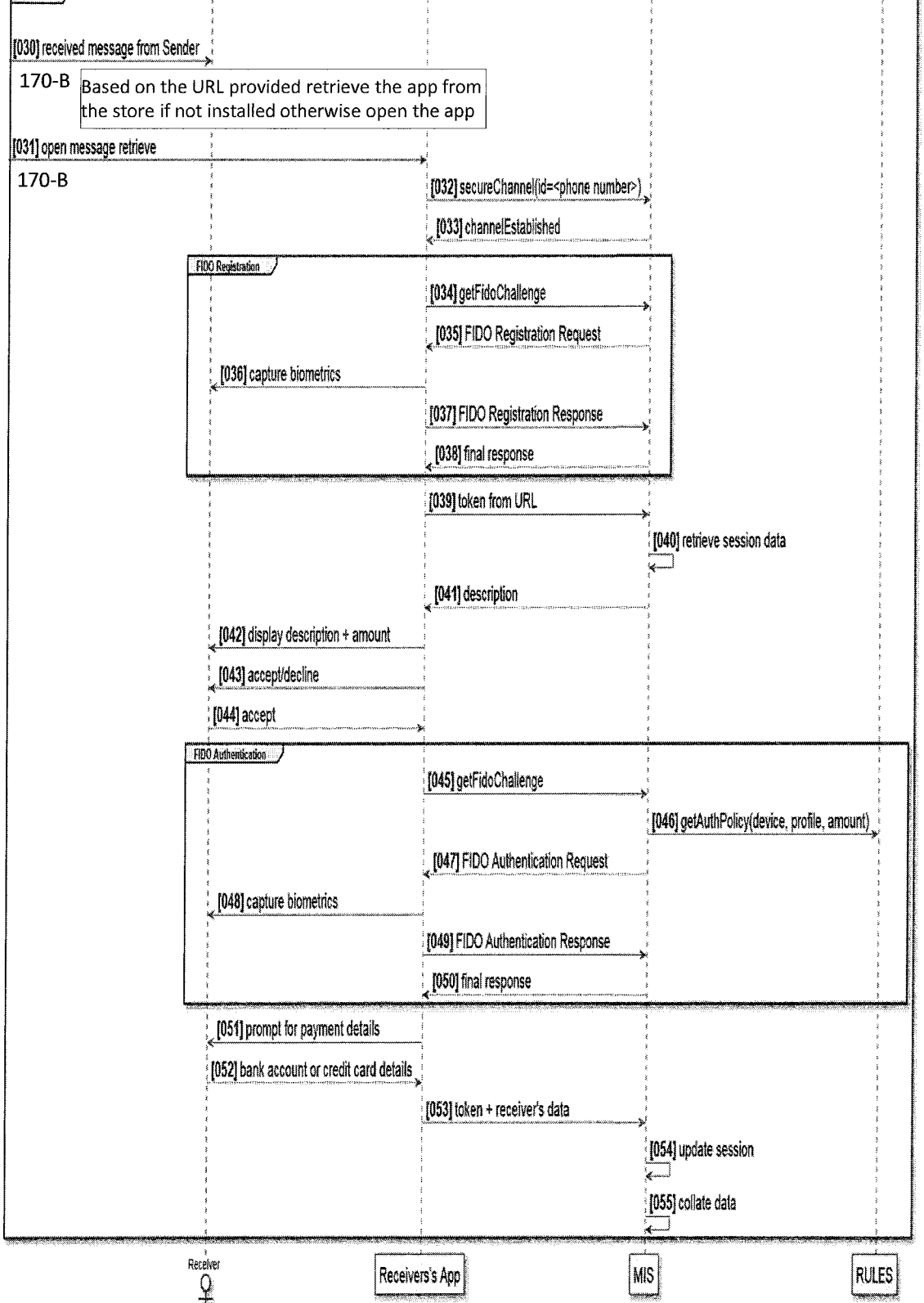
Receiver
100-B
Receivers's App
120
MIS
130
RULES
Receiver
[030] received message from Sender
170-B
Based on the URL provided retrieve the app from the store if not installed otherwise open the app
[031] open message retrieve
170-B
[032] secureChannel(id=<phone number>)
[033] channelEstablished
FIDO Registration
[034] getFidoChallenge
[035] FIDO Registration Request
[036] capture biometrics
[037] FIDO Registration Response
[038] final response
[039] token from URL
[040] retrieve session data
[041] description
[042] display description + amount
[043] accept/decline
[044] accept
FIDO Authentication
[045] getFidoChallenge
[046] getAuthPolicy(device, profile, amount)
[047] FIDO Authentication Request
[048] capture biometrics
[049] FIDO Authentication Response
[050] final response
[051] prompt for payment details
[052] bank account or credit card details
[053] token + receiver's data
[054] update session
[055] collate data
Receiver
Receivers's App
MIS
RULES

Figure 3

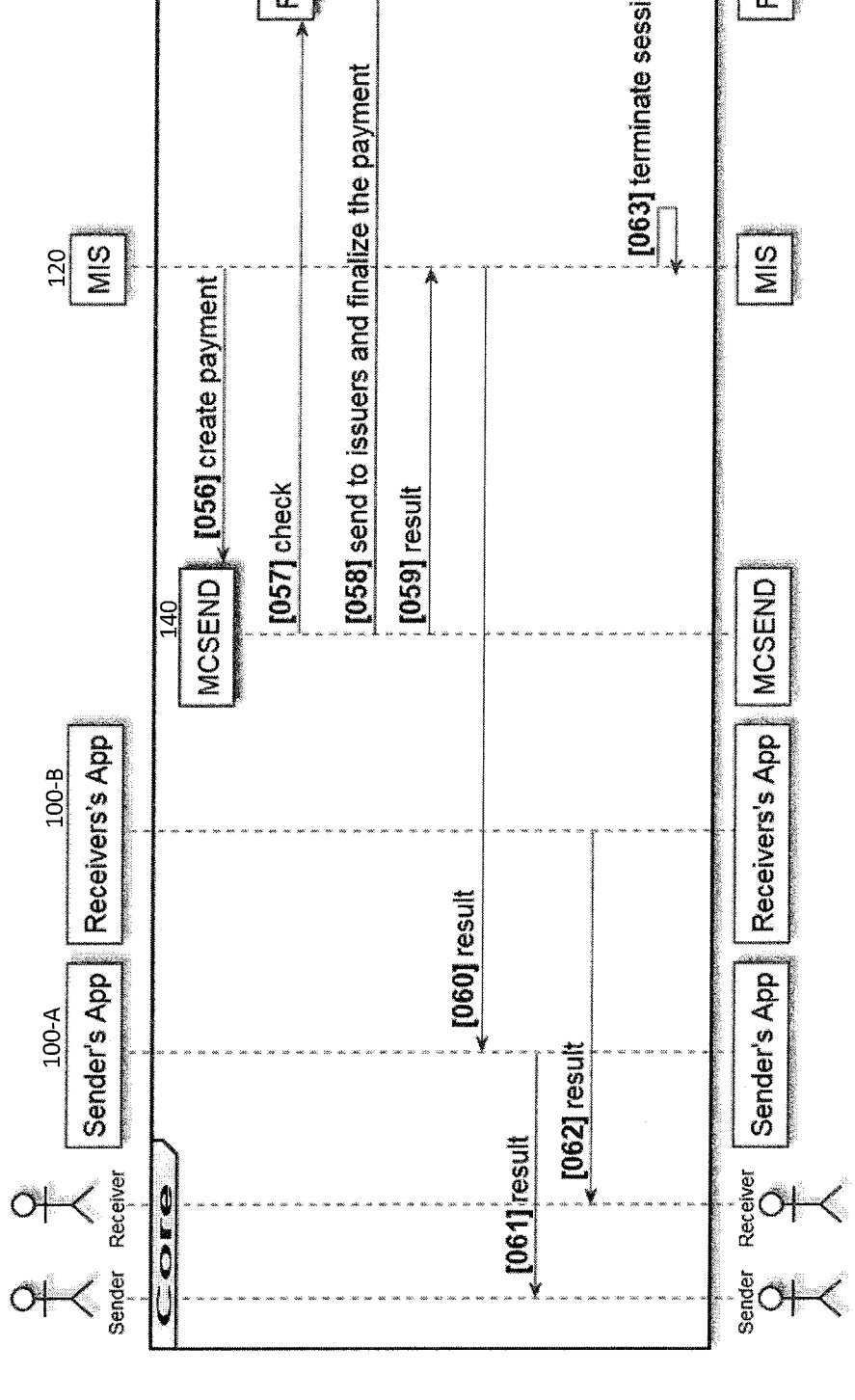
Sender
Receiver
core
100-A
Sender's App
100-B
Receivers's App
120
MIS
140
MCSEND
160
FRAUD
150
[056] create payment
[057] check
[058] send to issuers and finalize the payment
[059] result
[060] result
[061] result
[062] result
[063] terminate session
FRAUD
MIS
MCSEND
Receivers's App
Sender's App
Receiver
Sender

Figure 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/053293

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/00
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 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 2016/328700 A1 (BORTOLOTTO PAOLO [SG] ET AL) 10 November 2016 (2016-11-10) abstract paragraph [0092] paragraph [0098] - paragraph [0099] paragraph [0100] paragraph [0104] paragraph [0119] paragraph [0122] paragraph [0124] paragraph [0126] paragraph [0136] figures 1, 2, 3	1-14

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 November 2018	21/11/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Stark, Konrad

1

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/238492 A1 (MUTHU SRI SARAVANA [US] ET AL) 12 September 2013 (2013-09-12) abstract paragraph [0017] - paragraph [0040] paragraph [0057] - paragraph [0063] figures 1, 3A, 3B -----	1-14
X	US 2015/278816 A1 (FLEISHMAN JACK [CA] ET AL) 1 October 2015 (2015-10-01) abstract paragraph [0090] - paragraph [0097] figures 7, 8, 9a, 9b, 13, 17 -----	1-14
X	Fido Alliance: "FIDO UAF Architectural Overview", , 2 February 2017 (2017-02-02), XP055434553, Retrieved from the Internet: URL:https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-overview-v1.1-id-20170202.pdf [retrieved on 2017-12-12] the whole document -----	1-14

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2018/053293

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016328700 A1	10-11-2016	AU 2016257858 A1	23-11-2017
		CA 2985066 A1	10-11-2016
		CN 107851255 A	27-03-2018
		EP 3091492 A1	09-11-2016
		US 2016328700 A1	10-11-2016
		WO 2016179165 A1	10-11-2016
US 2013238492 A1	12-09-2013	NONE	
US 2015278816 A1	01-10-2015	CA 2332656 A1	26-07-2002
		GB 2389443 A	10-12-2003
		MX PA03006777 A	08-04-2005
		US 2004148252 A1	29-07-2004
		US 2011125644 A1	26-05-2011
		US 2015278816 A1	01-10-2015
		WO 02059847 A1	01-08-2002