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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 October 2014 (09.10.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/162113 A2

(51) International Patent Classification:
G06F 21/31 (2013.01)

(21) International Application Number:
PCT/GB2014/051000

(22) International Filing Date:
28 March 2014 (28.03.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1306016.5 3 April 2013 (03.04.2013) GB

(71) Applicant: **CLOUDZYNC LTD** [GB/GB]; New North House, 4th Floor, 78 Ongar Road, Brentwood Essex CM15 9BB (GB).

(72) Inventors: **SMITH, Andrew William**; 24 Edwards Way, Hutton, Brentwood Essex CM13 1BT (GB). **SEDDON, Mark Earl**; 25 Park Way, Shenfield, Brentwood Essex CM15 8LH (GB).

(74) Agent: **KILBURN & STRODE LLP**; 20 Red Lion Street, London, Greater London, WC1R 4PJ (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) Title: SECURE COMMUNICATIONS SYSTEM

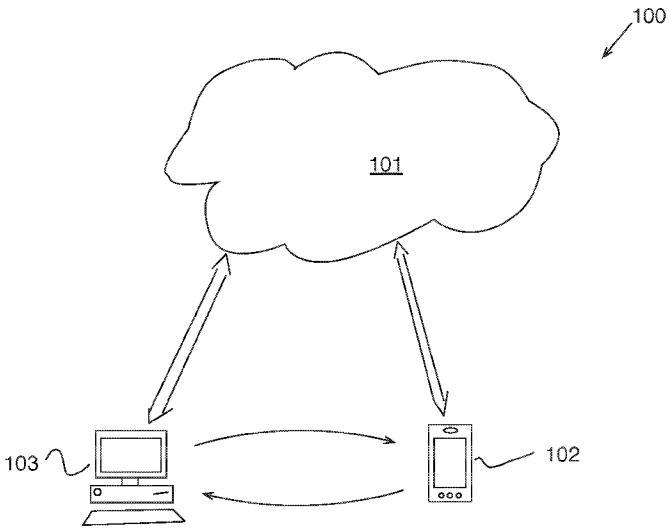


Figure 1

(57) Abstract: A method, apparatus and computer readable medium for providing secure communication between a plurality of parties is disclosed. The method comprises: receiving, at an authorisation system, a first communication from a first party, the first communication comprising information identifying a second party to which the first communication is directed; verifying, at the authorisation system, an identity of the first party; sending, from the authorisation system when the identity of the first party is verified, a second communication to the second party in accordance with the first communication; receiving, at the authorisation system, a third communication from the second party issued in response to the second communication; and verifying an identity of the second party responsive to receipt of the third communication.

WO 2014/162113 A2

Secure Communications System

Field of Invention

This disclosure relates to a system that provides for secure communications between two or more parties. More specifically, but not exclusively, a security system is provided through which communications between a plurality of communicating parties pass. Due to the security functionality provided by the secure communications system, the system is particularly useful for processing and managing financial transactions.

Background to the Invention

For over 50 years, the use of bank cards such as debit and credit cards have formed part of a preferred system for making payments. Bank cards reduce the need for people to carry large sums of money on their person, while providing the owner or user associated with the card with the ability to make payments. Nowadays, such cards work by having personal identification information stored on the card, generally in a magnetic strip formed on the card or a microchip embedded in the card, which is used to identify a bank account from which payment can be taken. However, since bank cards provide access to persons bank account, there are risks regarding security. In particular, there is a risk that if a bank card gets lost or stolen someone other than the owner of the card may be able to obtain access to the card owner's bank account. Furthermore, bank cards can be replicated relatively easily, therefore leading to further security risks. In the past, replication of a signature on the back of a card has been used to verify the identity of the user of the bank card. However, such security provisions were deemed insufficient a number of years ago. It then became common for a 4-digit PIN number in accordance with so-called smartcard technology to be used as a means of providing security in the use of bank cards. However, bank card identity theft is still a major problem, particularly due to the rise of using details provided on bank cards to make payments online. Hence, there is a continuing need to further improve security provisions associated with bank cards.

The concept of bank cards, wherein a card is used as a link to an account, has been extended to other applications. Loyalty cards are one such example. A loyalty card is a card associated with a loyalty account. Whenever a consumer that has such a loyalty card makes a purchase at a store having a loyalty scheme with which the card is associated, the consumer's loyalty card is read by a card reader and based on information obtained by the card reader identifying the card and the purchase made,

loyalty points are added to the loyalty account associated with loyalty card. Stores will then often provide vouchers to the consumer associated with the loyalty card, the value of such vouchers depending on the number of points obtained.

Most stores have their own loyalty point scheme and it is therefore common for consumers to need to carry all of their loyalty cards for all of the stores that they shop at within their wallet or purse in order for them to use such loyalty schemes.

It is therefore common that due to consumers having a number of different bank cards, such as one or more debit cards and one or more credit cards, in addition to many loyalty cards, consumers wallets are getting overloaded with cards. This results in consumers having to carry very large wallets around with them at all times, or only carry a select number of cards with them, which may mean that they lose out on loyalty points in certain stores.

There are therefore various problems associated with user cards that currently remain unresolved.

Summary of Invention

In accordance with an aspect of the invention there is provided a method for providing secure communication between a plurality of parties. The method comprises receiving, at an authorisation system, a first communication from a first party. The first communication comprises information identifying a second party to which the first communication is directed. The method further comprises verifying, at the authorisation system, an identity of the first part. Furthermore, the method comprises sending, from the authorisation system when the identity of the first party is verified, a second communication to the second party in accordance with the first communication. In addition, the method comprises receiving, at the authorisation system, a third communication from the second party issued in response to the second communication. The method also comprises verifying an identity of the second party responsive to receipt of the third communication.

The method may be for providing secure communication between a plurality of parties for processing a financial transaction between the plurality of parties.

The first party may be a merchant and the first communication may comprise information identifying the financial transaction to be processed. The second party

may be a consumer and the third communication may comprise information indicating that the second party approves the financial transaction.

The method may comprise processing the financial transaction when the authorisation system receives approval of the financial transaction from the second party and verifies the identity of the second party.

If the identity of either the first or second party is not successfully verified then the financial transaction may be cancelled.

The first communication may comprise information identifying the merchant. The method may further comprise identifying if the consumer has a loyalty account with the merchant. The method may also further comprise sending, if the consumer has a loyalty account with the merchant, a fourth communication to the merchant comprising information identifying the consumer's loyalty account with the merchant and information identifying the financial transaction for the merchant to add loyalty points to the consumer's loyalty account with the merchant.

The method may further comprise determining, at the authorisation system, the identity of the second party from the information identifying the second party provided in the first communication.

The method may further comprise receiving location information indicative of a location of the second party. Furthermore, the method may further comprise determining if the location information is indicative of fraudulent activity.

The method may further comprise receiving location information indicative of a location of the first party. Determining if the location information is indicative of fraudulent activity may comprise comparing the location information indicative of a location of the first party with the location information indicative of a location of the second party.

Determining if the location information is indicative of fraudulent activity may further comprise comparing the location information indicative of a location of the second party with information indicative of a previous location of the second party.

The method may further comprise creating a profile of the second party, the profile indicative of characteristics of the second party. In addition, the method may comprise determining current characteristics of the second party. The method may also comprise comparing the profile of the second party with the current characteristics of the second party. The method may also comprise identifying the presence of fraudulent activity by the second party in accordance with the comparison of the profile.

The characteristics of the second party include location information associated with the second party.

The method further comprises receiving, with the third communication, information indicative of the current characteristics of the second party.

The identity of the first and second parties may be verified in accordance with information provided in the first and third communications respectively.

The information provided in the third communication may be security information. The identity of the second party may be verified by comparing the security information received in the third communication with security information stored in a memory of the authorisation system.

The security information may comprise information identifying a device being used by the third party and information identifying the third party using the device. The information identifying a device used by the third party may comprise one or more of: information identifying hardware of the device; information identifying the type of the device; information identifying an operating system used by the device; information identifying a version of the operating system of the device; and a UDID or Unique ID of the device. The information identifying the third party using the device may comprise one or more of an OAuth identifier and a PIN code.

The information identifying a device being used by the third party and information identifying the third party using the device may be encrypted using an encryption process to form the security information.

An item of the information identifying the device being used by the third party or an item of information identifying the third party using the device may be used as an

encryption key for producing the encrypted fingerprint. A PIN code associated with the third party may be used as the encryption key.

Verifying the identity of the first party may comprise determining if the first party is registered with the authorisation system.

According to another aspect of the invention apparatus for providing secure communication between a plurality of parties is provided. The apparatus comprises a communication for communicating with a plurality of parties, and a processor arranged to process information. The apparatus is arranged to perform any method for providing secure communication between a plurality of parties as described herein. The apparatus may be a cloud-based server arrangement.

According to a further aspect of the invention a method for verifying validity of communications is provided. The method comprises receiving a communication from a device associated with a user, the communication comprising information identifying the device associated with the user and information for verifying an identity of the user associated with the device. The method also comprises determining if the device is a device registered for use by the user of the device. In addition, the method comprises verifying if the user is the registered user of the device.

The method may further comprise performing further processing associated with the communication if the device is determined to be registered for use by the user of the device and the user is verified as the registered user of the device. For example, the further processing could be the processing of a financial transaction, or the enabling of the initiation of a direct communication channel.

The communication may comprise information identifying a second user to which the communication is directed. The further processing associated with the communication may comprise sending a communication to the second user.

Determining if the device is a device registered for use by the user of the device may comprise comparing information identifying the device associated with the user with information identifying the device associated with the user stored in a memory of an authorisation system performing the verification. The information identifying the device associated with the user may comprise one or more of information identifying

hardware of the device, information identifying the type of the device, information identifying an operating system used by the device, information identifying a version of the operating system of the device, and a UDID or Unique ID of the device.

Determining if the user is the registered user of the device may comprise comparing information for verifying an identity of the user associated with the device with information for verifying an identifying of the user associated with the device stored in a memory of an authorisation system performing the verification. The information for verifying an identity of the user associated with the device may comprise one or more of an OAuth identifier, and a PIN code.

The information identifying the device associated with the user and information for verifying an identifying of the user associated with the device may be received as an encrypted fingerprint providing an individual identifier of the user at the user device.

An item of the information identifying the device associated with the user or an item of information for verifying an identifying of the user associated with the device may be used as an encryption key for producing the encrypted fingerprint. A PIN code associated with the user may be used as the encryption key.

The method may be for verifying the validity of communications for use in processing of financial transactions.

According to another aspect of the invention apparatus for verifying validity of communications is provided. The apparatus comprises a communication unit for communicating with a plurality of parties and a processor arranged to process information. The apparatus is arranged to perform any method for verifying validity of communications disclosed herein. The apparatus may be a cloud-based server arrangement.

According to yet another aspect of the invention there is provided a method for producing security information to be associated with a communication, the security information for verifying the validity of the communication. The method comprises obtaining information identifying a device associated with a user and information for verifying an identity of the user associated with the device. The method also comprises producing security information in accordance with the information

identifying a device associated with a user and information for verifying an identity of the user associated with the device.

The method may further comprise encapsulating the security information in a communication to be sent by the user device. The security information may be encapsulated within a header of the communication.

The information identifying the device associated with the user may comprise one or more of information identifying hardware of the device, information identifying the type of the device, information identifying an operating system used by the device, information identifying a version of the operating system of the device, and a UDID or Unique ID of the device.

The information for verifying an identity of the user associated with the device comprises one or more of an OAuth identifier and a PIN code. The security information may be produced by encrypting the information identifying the device associated with the user and the information for verifying an identity of the user associated with the device.

An item of the information identifying the device associated with the user or an item of information for verifying an identity of the user associated with the device may be used as an encryption key for producing the encrypted security information. A PIN code associated with the user may be used as the encryption key. The security information may be a fingerprint. The fingerprint may be provided in any form as described herein.

According to another aspect of the invention apparatus for producing security information to be associated with a communication, the security information for verifying the validity of the communication. The apparatus comprises a processor arranged to perform any method for producing security information to be associated with a communication, the security information for verifying the validity of the communication as disclosed herein. The apparatus may be a smart phone.

According to yet a further aspect of the invention there is provided a method for preparing a packet for secure and efficient transmittal over a network. The method comprises inserting content to be transmitted over a network within a body of a packet. The method also comprises inserting security information for authentication

purposes within a header of the packet. The security information may be produced in accordance with any appropriate method described herein. The method may further comprise transmitting the packet to a recipient.

According to another aspect of the invention apparatus for preparing a packet for secure and efficient transmittal over a network is provided. The apparatus comprises a processor arranged to perform any method for preparing a packet for secure and efficient transmittal over a network as disclosed herein.

According to yet another aspect of the invention a method for verifying the validity of information received over a network is provided. The method comprises receiving, over a network, a packet comprising content within a body of the packet and security information for authentication purposes within a header of the packet. The method also comprises obtaining, from the header of the packet, the security information. The method also comprises verifying the received packet in accordance with the security information. The verification may be performed in any suitable way as described herein. It will be appreciated that the packet referred to may also be referred to as a communication herein. The security information referred to may also be referred to as the information identifying the device associated with the user and the information for verifying an identity of the user associated with the device.

According to a further aspect of the invention a method for routing communications from a source to one or more recipients may be provided. The method comprises determining a respective communication channel for sending content received from a source to each of one or more recipients. The method also comprises sending a communication including the content to the one or more recipients using the respective communication channel.

The step of determining a respective communication channel may further comprise determining a device associated with each recipient, determining a device type of the device associated with each recipient, and determining the respective communication channel for sending the content to each of the one or more recipients in accordance with the device type for the respective recipient. The respective communication channel may be a protocol associated with the device type. The protocol may be a communication protocol for communicating with the device type using one of the following operating systems: iOS, Android, or Windows Phone.

The method may further comprise receiving, from the source, the content to be sent to the one or more recipients and the information identifying the one or more recipients. The content to be sent to one or more recipients and the information identifying the one or more recipients may be received in a single communication.

The method may further comprise receiving information identifying the one or more recipients, prior to determining a respective communication channel for each of the one or more recipients, in accordance with location information associated with the one or more recipients. The recipients may be identified in accordance with location information when it is determined, from the location information that the one or more recipients are within a predetermined distance of a location associated with the source.

The method may further comprise receiving a request from the one or more recipients for information from the source prior to determining a respective communication channel for sending the content received from the source to each of the one or more recipients.

The method may further comprise receiving a request from the one or more recipients for a type of information. In addition the method may further comprise requesting the type of information from one or more sources including the source. The method may also comprise receiving the content from the source responsive to the request for the type of information. The method may be performed at or by a data processing system.

According another aspect of the invention apparatus for routing communications from a source to one or more recipients is provided. The apparatus comprises a communication unit for communicating with a plurality of parties. The apparatus also comprises a processor arranged to process information. The apparatus is also arranged to perform any method for routing communications from a source to one or more recipients as disclosed herein. The apparatus may be a cloud-based server arrangement.

According to a further aspect of the invention a method for setting up a communication channel is provided. The method may comprise receiving, at a data processing system, a communication from a first party. The communication comprises information indicative of a communication channel to be set-up from the

data processing system to a second party. The method further comprises setting-up, at the data processing system, a communication channel in accordance with the information indicative of a communication channel to be set-up.

The second party may be arranged to communicate with parties communicatively coupled to the data processing system through the communication channel. The information indicative of a communication channel to be set-up may comprise a communication channel definition. The method may further comprise producing, at the data processing system, a communication channel definition in accordance with the information indicative of a communication channel to be set-up. The information indicative of a communication channel to be set-up may comprise information for the data processing system to identify the second party for setting-up the communication channel from the data processing system to the second party.

The communication channel definition may comprise a definition of an API end point associated with the second party. The API end point may be a RESTful API end point. The communication channel definition may further comprise a return API definition that defines a channel for communications to be transmitted from the second party to the data processing system. The communication channel definition may further comprise content to be transmitted to the second party.

The content to be transmitted to the second party may include required data capture information to be obtained from a third party by the second party. The data processing system may verify all communications from parties passing through the data processing system.

According to another aspect of the invention there is provided apparatus for setting up a communication channel. The apparatus comprises a communication unit for communicating with a plurality of parties. The apparatus also comprises a processor arranged to process information. The apparatus is arranged to perform any method for setting up a communication channel as disclosed herein. The apparatus may be a cloud-based server arrangement.

According to yet another aspect of the invention a method for creating a communication channel definition for setting up a communication channel between a data processing system and a party is provided. The method comprises producing, at a first party, information indicative of a communication channel to be set-up from a

data processing system to a second party. The method further comprises transmitting, from the first party to the data processing system, a communication comprising the information indicative of a communication channel to be set-up from the data processing system to a second party for the data processing system to set-up the communication channel.

The method may further comprise creating, at a first party, a communication channel definition. The communication channel definition may be arranged to define a communication channel from a data processing system to a second party. The information may be indicative of a communication channel to be set-up comprises the communication channel definition. The communication channel definition may comprise a definition of an API end point associated with the second party. The API end point may be a RESTful API end point. The communication channel definition may further comprise a return API definition that defines a channel for communications to be transmitted from the second party to the data processing system.

The communication channel definition may further comprise content to be transmitted to the second party. The content to be transmitted to the second party may include required data capture information to be obtained from a third party by the second party. The information indicative of a communication channel to be set-up may comprise information for the data processing system to identify the second party for setting-up the communication channel from the data processing system to the second party.

According to a further aspect of the invention the apparatus for creating a communication channel definition for setting up a communication channel between a data processing system and a party is provided. The apparatus comprises a communication unit for communicating with a data processing system. The apparatus also comprises a processor arranged to process information. The apparatus is arranged to perform any method for creating a communication channel definition for setting up a communication channel between a data processing system and a party as described herein.

According to yet a further aspect of the invention a method for controlling a quantity of cloud-based resources utilised by a system is provided . The method comprises determining a quantity of cloud-based resources required by a system. The method

further comprises adjusting a current quantity of cloud-based resources associated with the system in accordance with the determined quantity of cloud-based resources required by the system.

The method may further comprise monitoring usage characteristics of the current quantity of cloud-based resources associated with the system. The quantity of cloud-based resources required by the system may be determined in accordance with the monitored usage characteristics. The current quantity of cloud-based resources may comprise a plurality of servers arranged within a cloud structure. The usage characteristics of each of the plurality of servers may be monitored. The monitored usage characteristics may include one or more of database loads, average web server request, and latency.

The method may further comprise creating a profile of characteristics of usage of the system over time. The quantity of cloud-based resources required by the system may be determined in accordance with the profile.

The method may further comprise predicting a future usage of the cloud-based resources associated with the system, where the quantity of cloud-based resources required by the system is determined in accordance with the prediction of future usage. The the future usage of the cloud based resource may be predicted based on known characteristics of a future time.

The method may further comprise determining the adjustment of the current quantity of cloud-based resources by comparing the determined quantity of cloud-based resources and the current quantity of cloud-based resources.

The current quantity of cloud based resources may be adjusted by sending a message to a provider of the cloud-based resources requesting that the current quantity of cloud-based resources be adjusted in accordance with the adjustment of the current cloud-based resources.

According to another aspect of the invention there is provided apparatus for controlling a quantity of cloud-based resources utilised by a system. The apparatus comprises a processor arranged to perform any method for controlling a quantity of cloud-based resources utilised by a system disclosed herein.

The apparatus may further comprise a communication unit arranged to provide communication functionality as described herein. The apparatus may further comprise a monitoring arrangement arranged to monitor usage characteristics of the current quantity of cloud-based resources as described herein.

According to another aspect of the invention a method for processing items having associated content for being displayed is disclosed. The method comprises obtaining a plurality of items having associated content for being displayed in a plurality of cells forming a cell structure of a user interface. The plurality of items may be obtained from a memory. The method further comprises analysing the plurality of items to determine a number of cells of the cell structure required to display the content associated with the respective item. The method also comprises determining which of the plurality of items to display the respective content of in the cell structure based on the cell structure and the determined number of cells required to display the content associated with each of the plurality of items. Furthermore, the method comprises displaying, in the cell structure, the content associated with the determined items of the plurality of items to be displayed.

The cell structure may comprise a number of cells. The determining which of the plurality of items to display the respective content of in the cell structure may comprise comparing the number of cells required to display the information for each of the plurality of items and the number of cells in the cell structure.

The number of cells in the cell structure may be arranged in a two-dimensional array. The determining which of the plurality of items to display respective content of in the cell structure may comprise comparing the number of cells required to display the content associated with each of the plurality of items and the cell structure of the two-dimensional array of cells.

The plurality of cells required to display the content may be set according to a type of the content associated with the respective item. The analysing may comprise determining the type of the content associated with each of the respective items. The method may further comprise grouping the plurality of items according to type of the content associated with the respective items. The determining which of the plurality of items is to have its associated content displayed may be carried out on a group of the plurality of items corresponding to the type of the content. The type of

the content may be determined from a code indicative of the type of the content associated with the item. The type of the content may be one of vouchers, loyalty scheme updates, personalised deals, tickets, electronic receipts, warranties, and travel documentation.

According to another aspect of the invention there is provided apparatus for processing items having content for being displayed. The apparatus comprises a memory arranged to store a plurality of items having associated content for being displayed in a cell structure of a user interface. The apparatus also comprises a processor arranged to perform any method for processing items having content for being displayed disclosed herein. The apparatus also comprises a display arranged to display content associated with items that the processor determines are to be displayed.

According to another aspect of the invention a computer readable medium comprising computer readable code operable, in use, to instruct a computer system to perform any method disclosed herein is provided.

In certain arrangements of the system, each device that is arranged to connect to the service provider system is uniquely identifiable for every single communication exchange between the service provider system and a calling device. In such arrangements, the amount of data to be transferred across a network for such communications is dramatically reduced when compared to state of the art systems.

Arrangements are disclosed that provide a unique protocol that enables efficient and secure communication between a calling device and a service provider system. This efficient and secure communication may be provided for every single communication request. This protocol may allow for greater security between a calling device and service provider system, while reducing the amount of data passed across a communication network thereby improving network and data transfer efficiency.

In some implementations disclosed herein an application is installed in a user device for providing functionality disclosed herein. This application may create a unique digital fingerprint of the device. The digital fingerprint may be based on hardware and/or software specifications of the user device, and optionally in addition to a configuration of the device. Furthermore, the fingerprint may include specific information related to the user associated with the device. The user associated with

the device may be a user registered with the service provider system for using the device. The user information may derive from login information provided by the user. For example, the login could be provided via a supported OAuth protocol such as Facebook, Windows Live, or Google. The fingerprint identifier may be stored on the device and in the service provider system or 'cloud'.

A method is disclosed wherein a device initiates communication and then sends this communication directly to the service provider cloud, along with identification data of a second device to communicate with. For example, this may be the second device's mobile number. The communicated instruction is then sent to the second device, where it is displayed on the device screen hardware and requires a user interaction at the second device. The user's input and required communication data is then passed back to the service provider cloud, allowing the service provider cloud to complete the action requested. The cloud then completes the operation and returns the result to both devices.

In at least some implementations, additional information can be associated with a transaction being processed. Such additional information may include one or more of a voucher and/or loyalty scheme data. All of this information can be provided in a single communication call.

In certain implementations disclosed herein a "merchant" can issue direct messages to users registered on the service provider system. In this scenario, the merchant does not need to support multiple device operating systems or understand the individual devices the users may be using. Furthermore, the merchant does not need to have an application installed on the end users mobile device. Instead, just a single call is required identifying information to be sent to one or more recipients, also identified in the call, and the service provider system then delivers the information or content to the required recipients. This reduces the need to manage multiple language, operating systems, and hardware for content delivery and use. Instead the service provider system provides this functionality. Furthermore, such implementations enable developers to use any development language in order to deliver content and operating specific notifications to one or more mobile devices. The requirement for content and notification originators to have their own application installed on the end users mobile device is also removed. Content and single notifications can therefore be distributed to any device – there are no restraints based on hardware or device operating system.

Brief Description of the Drawings

Exemplary embodiments of the invention shall now be described with reference to the drawings in which:

Figure 1 shows a secure communications environment in accordance with an embodiment of the invention;

Figure 2 is a flow diagram of a procedure for completing a financial transaction using the secure communications environment of Figure 1;

Figure 3 shows a system in which a third party server is incorporated into the secure communications environment shown in Figure 1 using a workflow functionality;

Figure 4 is a flow diagram of a procedure for introducing a third party into the secure communications environment as shown in Figure 3 in an exemplary embodiment wherein the third party is the issuer of a warranty; and

Figure 5 shows a homepage screen for the app installed on the user device shown in Figure 1.

Throughout the description and the drawings, like reference numerals refer to like parts.

Specific Description

Secure Communication System

A system is described herein that provides a mechanism for secure communications between two or more parties. The system has various applications, but the system shall initially be described with reference to an exemplary embodiment in which the secure communications system is used for processing of a financial transaction taking place between a user or a consumer and a merchant.

Figure 1 shows the secure communications environment 100 for processing of payments. The process works by providing a secure cloud-based system or server 101 that controls the payment process operated by the provider of the secure

payment service. This server is hereinafter referred to as the service provider system 101. When a user wants to complete a financial transaction from a merchant, e.g. the user wants to purchase an item from a shop associated with the merchant, the transaction is processed via user device 102 and merchant device 103 communicating through the service provider system 101. Since communications between the merchant device 103 and user device 102 take place through the service provider system 101 all communications can be subject to the security provisions provided by the server 101.

Each device that is to be connected to the service provider system 101, whether it be a merchant or user device, is uniquely identifiable, which is a requirement for the secure communication exchange provided by the service provider.

The service provider system 101 is shown as a cloud-based server. As will be described, the service provider system is arranged to dynamically use cloud resources provided by cloud-based servers. Such resources include processing and memory functionality. It will be appreciated that in alternative arrangements fixed rather than cloud-based servers are utilised.

The user device 102 is shown as a smart phone in Figure 1. In latter sections of this disclosure it will be appreciated that the user can also complete transactions using other devices such as a computer. However, the following description is based on the concept of the user using a smart phone.

In Figure 1, the merchant device 103 is shown as a computer. It will be appreciated that the merchant may have a plurality of devices at multiple locations and not just a single device. However, only a single terminal is shown for ease of explanation. Furthermore, the merchant may utilise another electronic device such a smart phone or cell phone-based device.

All communications between the merchant device 103 and user device 102 are primarily web-based communications, even though clearly at least part of the communications will also pass through the cellular mobile phone network for communicating with the user device 102.

The specific processes involved in making a transaction, and the associated security provisions, shall be now be explained.

Registration

In order for the user to purchase an item from the merchant within the environment 100, it is firstly necessary for both the user and the corresponding user device 102, in addition to the merchant and the corresponding merchant device 103 to be registered with the service provider system 101. This registration process shall now be discussed.

The merchant can register with the service provider system 101 providing the service provider system 101 with:

1) A Company number.
2) A VAT or other sales tax number.
3) Information relating to the geographical location of all of the merchants devices (e.g. the premises in which the devices are installed) that will be allowing payment using the system.

In different jurisdictions, there may be different requirements for merchant registration to comply with the requirements of local law.

This information can be provided via a web-based registration page.

The requirement of providing the geographical location of all of the merchant's stores or operational locations provides an additional level of security because any communications from the merchant must be from a specific merchant account if the transaction is an instore transaction type. Each device that the merchant wishes to use must sign into the merchant's user account, which is done via the merchant's own Active Directory or a shared / bespoke Active Directory provided by the service provider 101.

During the registration process the merchant is also able to select a level of service required from the service provider system 101. In particular, the merchant may only want to use the service provider system 101 for processing of payments. However, as will be discussed, there are various other functions that the service provider system 101 can provide, such as data pushing and loyalty point updating, and the merchant is therefore able to indicate which of the various services offered they would like to utilise.

Once the merchant has provided the service provider system 101 with sufficient information for setting up a merchant account with the service provider, the service provider system 101 stores this information in its memory and assigns a unique identifier for that merchant. To raise a transaction or use the system provider system 101, the merchant user must be "signed" into the system via Active Directory. Their Active Directory account informs the service provider system of the merchant account details and assigned merchant identifier.

The first step of the user registration process is for the user to download the service provider's app onto the user device 102. The registration process can then be performed using the app. Within the registration process provided by the app, the user is required to provide the following information:

a) Name.
b) Address.
c) Bank account details (optional).
d) OAuth identifier, e.g. Facebook login, Google login, Twitter Login, Live login
e) Information identifying the hardware and type of the user device e.g. Apple|iPhone 5, or WindowsPhone8|Nokia.
f) Device operating system, e.g. iOS, Android, or Windows Phone.
g) Device operating system version, e.g. iOS 6, Android ice cream sandwich, or Windows Phone 8 (build revision information is also collected, e.g. iOS 6.2.1.3).
h) Device UDID or Unique ID (proprietary or devised).
i) Channel URI / Device Token, this is a unique identifier that is required for push notifications for the specific device and its operating system.
j) User defined PIN code entered via the hardware of the device, this could be any 4-8 digit long number. Alternatively, an alpha-numeric password could be provided.

The information associated with points a), b), c), and j) can be input by the user into the service provider's app installed on the user device 102. The information set-out at point d) is captured once the user has signed into that OAuth provider. The information associated with each of e), f), g) and h) are automatically extracted by the service provider's app from the user device 102.

The bank account details c) are provided to provide the user's account with the service provider with funds for paying for a transaction. In one implementation, the user pays, from their bank account, a set amount of money, e.g. £50 into their account held by the service provider. This money is then used for transactions until that money runs out. The user is then required to add more funds to their account. In alternative implementations, the system can automatically add funds from the user's personal bank account to the user's account with the service provider. In yet further alternative implementations, the service provider may have a direct debit set-up with the user's personal bank so that all transactions that are authorised by the service provider are then debited from the user's personal bank account. Alternatively, the service provider account may be set up using a credit based structure, wherein the user is invoiced monthly for their transactions.

From the OAuth information the service provider system may be able to download a photo of the user, e.g. from facebook. Alternatively, the user may upload a photo of themselves to the system 101. As will be discussed, the photo can be used by a merchant as an additional security provision.

The PIN code is set by the user at registration. The PIN has to be input by the user every time they log into the application. As will be seen, this means that payments cannot be approved without the user inputting the PIN. In alternative arrangements the PIN is not required to access the application, but is instead just required to approve a payment. During the registration process, or at a later time, the user can register additional devices for use with his/her account. For example a computer or work smart phone could be registered for use.

Fingerprint

The next step after the user registration process is for the user app to create a device fingerprint. The device fingerprint is a unique identification of the user and associated user device. The fingerprint is a security measure that is always required for a user device to communicate with and through the service provider system 101.

The device fingerprint is created by using the information listed at items a) to j), obtained during the user registration process. In alternative arrangements, only some of the information listed at items a) to j) may be used. This information is encrypted into a unique identifier for the user and the specific device. A key characteristic of the unique identifier is that it is specific to the user and the specific

user device, which provides improved security over current financial transaction security. In other words, for someone to use the user's funds stored in the user account held with the service provider, both the registered user device and user specific information must be obtained.

The device fingerprint is created by creating a SHA Hash value for the user's PIN and one or more raw data values of the fingerprint. The PIN is taken to increase the level of security, and adding a unique component based on the user to the fingerprint encryption. The PIN hash is then taken and a fixed Salt is added. The fixed Salt is generated in the user device 102 by the app. The fixed Salt may change with each release of the app. RFC 2898 is then used to derive a password Key. The result is then UTF 8 encoded. A HEX encode is then taken. The HEX encode becomes the encryption key for the device fingerprint raw data and can be either 128Bit, 256Bit, or 512Bit. The unique device ID is then encrypted with a derived key using one of the following algorithms: AES algorithm, Triple DeS, RC2, Blowfish, or Rijndael. The algorithm used to create the fingerprint can be changed periodically and at random intervals to further increase security. Finally, a Base 64 encoded output is provided. This output is stored as the complete device fingerprint identifier on the device and transmitted to service provider system 101 where it is also stored in the user's account information. The data that is encrypted enables the service provider 101 to check that device settings are not altered in any way, which therefore ensures greater levels of security. For example, if a PIN reset has been enforced within the app, it will break the fingerprint and therefore communication with the service provider 101 will not be valid.

The device fingerprint can be re-engineered by the service provider, i.e. decrypted. Decryption is required when the device itself is updated to use a new operating system, or a new version of the app is installed. In addition, a fingerprint maybe decrypted to retrieve data such as the users PIN. In this example, the users PIN is not stored on the service provider system 101, but is required to decrypt other stored data on the service provider system 101. Authentication can be checked from the decrypted fingerprint, as can authorisation data. Security levels can therefore be ensured. The derived data from the device fingerprint is also used in real time suspicious activity processes, that will be discussed.

If the user has multiple devices registered then each device has a unique fingerprint because the fingerprint depends on information specific to the device.

Once both the user device 102 and the service provider system 101 have the device fingerprint associated with the user device 102 stored in their memory, the device fingerprint is used as an authentication key for all future communications between these two devices, as will now be discussed.

The fingerprint provides particular security because the user's PIN is used as the encryption key or passcode, which means that decryption of the fingerprint and therefore obtaining the secure information that is encrypted is extremely difficult and only possible with the user's PIN. Furthermore, the multiple encryption stages further add to the difficulty of the fingerprint being decrypted to obtain the information that is encrypted.

Protocol

A proprietary protocol called the ZyncSign protocol is provided for secure communications between the user device 102 and the service provider system 101. The protocol enables communications from devices to the service provider system 101 to be authorised.

The ZyncSign protocol has a specific header set, which includes:

- A Base 64 encoded output. This holds identification data associated with the user device 102 and its associated user. In the example of financial transactions provided by the system provider 101, this identification data is the device fingerprint. However, in other configurations this identification data could be different to the device fingerprint.
- A defined schema specific to the protocol.
- A unique device identifying code – allocated to the device by the installed app at the time of registration.

For example, the header, using the ZyncSign protocol, could take the following form:

Authorization:
+v/+yZDiQ3t+alR7iHL3ACOcVc9lLSEqsePlBWQF0Z3k2ZNV1EOB+9Db2zu5zz/bC6
FjWenSclcOxl9eKrVOfQ==
ZyncWallet

CloudZyncDeviceId: 444555

All communications between any device and the service provider system 101 must use the ZyncSign protocol. Use of the ZyncSign protocol enables the service provider system to correctly identify the device, its state (if a valid device) and specific information such as the device operating system and build version, while also simplifying individual API service calls and reducing the amount of data passed in each call. This is because known security data is encapsulated in a single token which thereby ensures reduction in data transmitted over networks. Furthermore, the fact that the security data is encapsulated within the header means that there is such a reduction in data transmitted over networks. Not only does this reduce data loads on networks, but it also maintains higher levels of security during transactional calls to services because the security data is in an encrypted form even before the data is then transmitted over a secure https connection.

The ZyncSign protocol enables the service provider to check both user and device credentials on every single call. This is unique, as it enables the service provider to authenticate the user and authorise the hardware used to process the necessary calls. Typically, web based APIs use SOAP or other implementations. RESTful based APIs however provide nothing more than a unique URL. The ZyncSign protocol provides a security layer to every single REST based API call, without the calling service (or developer) having to add parameters to an API call.

Financial Processing Procedure

The procedure for completing a financial transaction at a merchant location, such as a store, shall now be described with reference to Figure 2.

When a customer goes to a till to buy a product in the merchant's store, the process starts by the merchant device 103 scanning a barcode of a product to be purchased. In response, the merchant device 103 initiates a communication and builds an initial data set at step 201. This data set includes information identifying the merchant and the item being purchased, or at least the financial value of the item being purchased. The merchant device 103 then initiates communication by sending out a message asking for the user device 102 to identify itself at step 201. This communication can be transmitted using near field communication (NFC) or similar short range communication protocols. The user device 102 then sends out a message identifying itself in response to the message from the merchant device 103 at step 202. In this

configuration the user device 102 must provide certain data that is sent as an encrypted block and includes:

- The user device unique id as allocated by the service provider during the registration process.
- A shared secret (a word and/or a number), taken from the registration data.
- A unique random generated number as derived by the device. This number is used as confirmation data at a later point in the transaction process.
- User Device 102 Latitude and Longitude co-ordinates.

The merchant device in this configuration is then able to identify the user device 102 from this message for this type of face to face transaction. It will be appreciated that the merchant device could identify the user device in other ways, for example, the user could show a unique identifier, such as a QR code, on a screen of the user device which is scanned by the merchant device 103. When using a QR code a time stamp may be generated to limit the length of time that the QR code is valid. Other ways of communicating between the devices could include the use of Bluetooth or infrared technology. When identifying the user device 202, the merchant device 103 obtains only the block of data. However, in alternative systems all the merchant need obtain is a single identifier for the user device 102 such as a mobile phone number associated with the user device 102. This alternative system is typically used when the merchant is unable to read data from the users device 102 (e.g. transactions made through a website or over the telephone). Such information is sufficient for the service provider system 101 to then identify the user.

At step 203, the merchant device 103 then joins the information identifying the user device 102 to the initial data set that was previously created. The combined information is then sent to the service provider system 101 via a secured HTTPS connection.

In response, to receiving the information from the merchant device 103, the service provider system 101 validates the identity of the merchant as will be discussed in more detail. In addition, the service provider system 101 determines who the registered user associated with the user device 102 is by comparing information stored on the service provider system 101 from the user registration process with the

information received from the merchant. The complete data set is then checked in real time for suspicious activity which will be discussed later.

At step 204, the service provider system 101 then sends the merchant device 103 additional security information about the user. This information may include one or more of:

- Name of the account holder of the device.
- Email address.
- Mobile phone number.
- Profile picture.

The user is then verified by the operator of merchant device 103 in accordance with this information. For example, the merchant could ask for additional identification or check that the profile picture received matches that of the person using the user device 102. Then, at step 205, the merchant device sends a communication to the service provider system 101 verifying the identity of the user. In alternative systems, steps 204 and 205 could be skipped. This would provide a simpler, but less secure system.

The service provider system 101 then stores information about the transaction in a temporary memory linking the user and the merchant together for the transaction while the transaction is being processed and generates a user approval message at step 206, which is sent to the user device 102. The user approval message provides the user with information regarding the amount of the transaction and requests the user to accept or decline the transaction. Since the user has to input their 8-digit pin to open to app, an additional level of security is provided for the user to authorise the payment.

Once the user approves the payment on the user device 102, a transaction approved message is sent from the user device 102 to the service provider system 101 at step 207. When the service provider system 101 receives the user approval, which it can verify was from the correct user and the correct user device from the fingerprint, the service provider system 101 can process the transaction. For example, the service provider system 101 can debit the user's account for the amount of the transaction. At this point the service provider system checks if the user has sufficient funds for the

transaction. This check could also be carried out after step 203. If the transaction is successfully processed, the service provider system 101 then sends a message confirming the transaction is complete to the user device 102 (step 208) and the merchant device 103 (step 209). This message includes a completed transaction authorisation code. The message to the user may be stored as a receipt in the user's account with the service provider.

The communication procedure for processing a financial transaction when a user is in store can also be applied to various other situations with minor modifications. For example, if a user is purchasing something over the Internet (e.g. from a website on a computer) or over the telephone, the user provides the merchant, via the Internet or telephone, with information identifying themselves. This information may be information such as name, address, and/or mobile phone number, which can then be sent onto the service provider system 101 by the merchant device 103 and used to identify the user. Hence, this procedure replaces steps 201, 202 and 203 of Figure 2, but after that the method can proceed in exactly the same way, with the user using a registered device to verify the financial transaction.

Suspicious Use Detection

The above-described financial transaction processing system has a number of in-built security provisions to help prevent and detect fraudulent transactions, this is known as the suspicious use detection. Suspicious use detection is split into a real time task and as a background task.

The real-time detection checks the validity of both parties, their data, their identifying devices and the authentication of the actual users in the transaction. In addition, the real-time detection checks against the capability of that user to complete the financial transaction, for example by analysing geographic location information.

More specifically, the real time task involves the service provider system 101 validating data provided by the communicating devices by comparing the received data to data stored on the service provider server prior to allowing a transaction to be completed. In particular, the following data is validated:

- The received fingerprint authentication data must match the corresponding data stored on the service provider server 101. In doing this, the service provider server is validating: the device based on data included in the

fingerprint identifying the specific device; and the user based on a pin number and an OAuth identifier, such as a facebook login.

- Once the device is identified, a check is carried out to make sure that all devices involved in the transaction are valid, i.e. the registration process was successfully completed and the device is listed as valid on the service provider system 101.
- The device must be correctly assigned to a valid account found on the service provider server 101.
- The device must be unique, i.e. there must not be a replicated device on the system.
- The communication type, e.g. face to face, online, or over the telephone, is identified by the merchant when the transaction is initiated. A check is then carried out to make sure that the transaction is of the type suggested. This procedure can use geographical data captured from the physical device that was included in the data sent to the service provider from the user device at the point of authorisation to determine if the geographical data falls within accepted parameters for the transaction type. For example, for a face to face transaction the user device and merchant device should be at the same location. Furthermore, for an online transaction the user device that approves the transaction should be at the same location as the computer via which the transaction is initiated to ensure that it is the same person making and approving the transaction. The location of the computer can be determined from an IP address.
- A further geographical check is carried out to ensure that the geographical data captured from the physical device does not exceed travel parameters for that user. In other words, it is determined whether or not the user could have travelled the distance between transactions in the time between transactions.

If the initiating device fails the suspicious use detection then all communications are stopped immediately and the device is banned. A procedure is provided for a user to unlock their account.

As mentioned in the description of Figure 2, the transaction processing procedure may include sending the merchant device 103 information about the user of the user device 102 for verification purposes. If the merchant does not believe that the person

using the user device is the valid user then they can send an instruction to the service provider system 101 to stop the transaction and ban the user device 102.

If the user has multiple devices registered to an account, the service provider system 101 sends the transaction approval message, i.e. step 206 in Figure 2, to all registered devices. If an additional device has been fraudulently registered with an account then the user will be able to tell from their validly registered device and inform the service provider system 101 accordingly.

If it is believed that an attempted transaction is fraudulent the geographic location information can assist in identifying the specific location of a fraudulent transaction.

The background detection involves monitoring user activity to form a pattern of usage or user profile. In addition, other data from the device and how it is utilised is captured and stored for reference. For example: input speed between the user and the device is recorded; and geographical data captured from the device is recorded from which movements and distances between communication points, as well as typical geographic locations for the device can be determined. Furthermore, the type of transactions can be analysed, such as use of a gym or a particular membership card or loyalty scheme. All of this information is incorporated into the user profile. A rules engine is deployed on the service provider system that monitors all captured data from devices and sources. The profile is then checked against new activity, such as a new financial transaction, to measure if the new transaction falls into the acceptable limits for that profile. If not, then the transaction can be suspended and the device / user activity can be suspended until validated.

The suspicious use detection methods described above improve the security of communications and transactions. Furthermore, these methods strengthen manual workflows and process checks by providing tangible information through mobile devices that enables end users to make informed decisions against. An example of this is that the merchant can check the picture of the registered user device against the physical person in front of them attempting to complete the financial transaction.

The service provider environment 100 provides additional functionality beyond financial transaction processing. The service provider environment also allows for loyalty point updating, use of vouchers for payment, the delivery of notifications such

as adverts, and setting up of workflows, for example for completing warranties. Each of these additional functionalities shall now be discussed.

Loyalty Point Updating

When a user makes a purchase from a merchant that has a loyalty scheme, the system is able to automatically add loyalty points to a user's loyalty points account held by the merchant.

Firstly, the user must register their loyalty scheme number for a merchant's loyalty scheme in their account on the service provider system 101. The user may perform this by inputting the data via a registered user device. Alternatively, the user could scan a loyalty card using a registered user device.

Loyalty points can then be assigned to the user when a financial transaction associated with the user is processed, as follows. Once a transaction between the user and a merchant is confirmed as being processed, the service provider system performs a check to determine if the user has any loyalty scheme registered in their account for the merchant. If the user does have a loyalty scheme registered, the service provider system then sends a communication to the merchant, that identifies the amount of the purchase and the user's loyalty scheme number. The merchant is then able to update their records regarding the user's loyalty points.

The loyalty point updating system provided by the service provider system 101 therefore removes the requirement for a user to carry a loyalty card, in addition the system removes the requirement for the user to even remember to indicate that they have a loyalty scheme with the merchant. Instead, the procedure is all carried out automatically.

Vouchers

The user account can store electronic vouchers. In particular, the user account can be considered an electronic wallet, which has not only a financial account for payments, but also stores vouchers.

In the transaction processing procedure of Figure 2, when the user is asked whether or not the user wishes to accept the transaction, if the user has a voucher(s) in the user account for the merchant from which they are purchasing, then any vouchers that are applicable can be either automatically added to the transaction, or in

alternative settings as configured by the user, that user can be prompted if they wish to use the voucher(s). If the value of the transaction is greater than the value of the voucher then the user is asked to approve payment by virtue of the voucher and the additional required funds. If the value of the transaction is less than the value of the voucher then the value of the voucher may be updated accordingly, but this will depend upon rules set by the merchant.

A user may add a voucher to their account by browsing available vouchers made available through the app installed on their registered device. These vouchers may be generally available vouchers or vouchers the merchant has distributed specifically to the user.

Alternatively a user may add a voucher to their account by scanning a physical voucher using the user device 102. The user device 102 will then send a message to the service provider system 101 using the ZyncSign protocol encapsulating information identifying the voucher. The service provider system 101 then communicates with the merchant that has issued the voucher to verify that the voucher is valid. If the voucher is valid the voucher is stored in the user account.

Vouchers can also be added to a user account when the user is purchasing something from a merchant's store. For example, if the user spends a certain amount of money with a merchant, this may trigger the issuance of a voucher. The merchant may send a communication identifying the voucher in response to receiving confirmation from the service provider system 101 that the transaction has been approved, i.e. in response to step 209 in Figure 2. There are many other ways in which a merchant can issue a user with an electronic voucher, for example, using the data pushing procedure discussed below.

Data Pushing

The service provider system is also able to provide a routing functionality for communications between devices registered with the service provider system. While this functionality has a broad range of applications, it will now be described with reference to an example of delivering advertisements from a merchant to one or multiple users.

A merchant is able to send adverts, such as limited offers in store, using the data pushing functionality of the service provider system. The ZyncSign protocol is used

to send content created by the merchant to the service provider system, which is then sent by the service provider system directly to one or more user devices, with the final communication from the service provider system to the user device using "push notifications" in the device specific operating system format, e.g. a Channel URI sent through to Microsofts Push Notifications service to deliver a push notification to devices that run Windows Phone 7, 7.5, 7.8 and 8.

The data pushing process shall now be described in detail.

When the user downloads the service provider mobile app onto the user device 102 a notifications URI is automatically created based on the device's operating system. This channel URI is securely stored on the user device and also transmitted to the service provider system 101. The service provider system 101 then stores this Channel URI and confirms the storage of the URI back to the device 102 so that the user device 102 does not continue to resend Channel URIs. Channel URIs are subject to change based on the operating system of the device, this means that they must be continually checked and kept in synchronisation with the service provider. The service provider system 101 also stores the URI. The storage of this Channel URI is in a separate storage location on a data storage server of the service provider system 101. This is because the service provider system 101 has a separate data schema and physical server (for security reasons) that has access to external cloud services to complete a push notification for a given device. Channel URIs are linked to individual devices as registered by a user. The service provider system 101 joins together the physical datasets of the user, the user's device fingerprint and the active Channel URI.

Since channel URIs change, in order for the service provider system 101 to remain in constant touch with the user device 102, and for the device 102 not to be orphaned, the application installed on a device 102 must check the hardware of the device 102 and detect any changes in the Channel URI, by checking its own internal storage. Any changes must be re-communicated back to the service provider system 101 as to ensure the device 102 is not orphaned from the device communications channel.

A merchant can push data to devices by sending the following information, to the service provider system 101:

- Information identifying one or more users for data to be pushed to. This could simply be a mobile phone number associated with a user, which the service provider system can then use to identify the user, or any other data that the service provider system could use to identify a user.
- A message to be sent to the one or more users identified. Hence, in this example advertising information may be sent. However, it will be appreciated that this could be any information that one party may wish to transmit to multiple parties.
- Optional referenced data. This could be a link to external data (via a URL) or could be data referenced within the system providers system 101, for example a link to a particular voucher defined in the system provider system 101

When the service provider receives this message, it firstly determines the user's identification in the message. For those users that can be identified and also have a device communication channel set up, the services provider system 101 is then able to prepare the messages to be sent to the user devices.

The service provider system 101 then creates messages for each different type of user device operating system, e.g. iOS, Android, Windows Phone etc, incorporating the content provided by the merchant into the messages. The service provider system 101 is then able to send the messages to each of the selected users using the correct operating system push notification protocol.

The service provider system 101 allows for great flexibility and accuracy of timely delivery. For example, the merchant can indicate when they want a message to be delivered, e.g. instantly, as soon as possible, or delayed until a specific date and time. Furthermore, the merchant can specify that they only want the message delivered when one of the identified users is at a specific location. For example, if a user is within a certain radius of the merchants shop on a certain day, an offer could be sent to the user device accordingly.

The advantage of this procedure is that device bound content can be distributed to specific devices in a highly efficient fashion without the calling services, such as the merchant, needing to know the device operating system or how notifications for given devices are handled. The URI registration process between each user device

and the service provider system sets up these channels of communication automatically. Furthermore, the calling services need not have an established direct link with the user devices themselves, but instead just have some information suitable for the service provider system to identify a respective user. Consequently, the calling service need not know anything about the device operating system, but deliver device operating system specific messages to a user device. Managing notifications and content distribution is therefore simple and highly efficient. Only a single call is required to distribute to multiple devices, supporting any device hardware and any device operating system.

The system is arranged so that users are able to block or filter pushed information by indicating on the mobile app on their registered user device 102. A message is then sent from the user device 102 to the service provider system 101 to set-up filtering parameters so that data originating from certain sources is blocked.

While the above example relates to a merchant pushing information to users, it will be appreciated that the service provider system 101 enables any registered device using any development language to distribute content to other registered devices no matter what the other devices operating system is.

In some systems, functionality is provided to enable data pushing responsive to a stimulus. For example, any mobile device within 1-mile of a particular store, for identified users, may be pushed a voucher on a particular day. These users are identified for these vouchers in advance, but the voucher is only distributed to the user once their device is within the given radius of a particular store. Alternatively, a user may indicate that they are travelling to Bristol for the day and would like any vouchers for use in Bristol. The service provider system is then able to send such a request out to all merchants then receive vouchers and distribute the received vouchers accordingly. Similarly, the user may indicate that they would like to buy a TV and request vouchers accordingly. Hence, there are various means for triggering the data pushing functionality.

Third Party Workflows

The service provider system is also able to process communications with third parties that are not registered with the service provider system 101. This is achieved by merging data sets from devices, accounts, businesses and suppliers using a workflow, as will now be discussed.

Using a workflow definition, the workflow functionality allows for any third party communication flow to be introduced into a merchant-consumer communication channel. More generally, a workflow is set-up by one business wanting to incorporate data from another business into a communication. This workflow is then sent to and used by the service provider system 101 to set-up the workflow. When setting up a workflow it is defined how the mobile device is to be used as a data capture/data reader device within a workflow. Furthermore, data required to be captured is also defined, as are the workflow steps and the end points of the workflow. In practice, a workflow definition tool used to define a workflow takes the form of an HTML5 based portal. Endpoints are dynamically generated within the service provider system based on an end point definition provided in the workflow definition. Endpoints can be used to expose a connection to third party workflows and datasets and to provide an end point to allow data and/or content to flow back into the service provider system 101 and seamlessly back down to the user device. A workflow definition is owned by its creator (who can be the service provider) or a specific business account holder.

The workflow functionality will now be described by means of an example shown in Figures 3 and 4. The following example shows how the third party workflow functionality can be used for completing a warranty. Figure 3 shows a system in which a third party server 104, in this case a manufacturer of a product bought by the user using user device 102 from a merchant using merchant device 103, is incorporated into the communication flow. Figure 4 shows the communication flow between the devices involved.

The process starts by a user going to a checkout to purchase a product. The merchant initiates the transaction by instructing the merchant device 103 of the purchase, this might be by scanning a barcode or such like. As with the description of Figure 2, a handshake then takes place where the merchant device 103 sends a user device request message 301 to which the user device responds 302. The merchant device 103 then prepares the data to be transmitted to the service provider server 103 for the next stages in processing the payment. At this point, the merchant device performs a check to determine if any additional workflows are required. In this example it is identified that a warranty workflow is required, i.e. a warranty is to be provided with the product being purchased. The process of setting up the workflow

shall now be described with reference to haw this process relates to the payment process of Figure 2 where necessary.

The merchant device 103 sends a pre-created workflow dataset to the service provider system 10 at step 303. This data can be encapsulated with the other transaction information being sent to the service provider system in order to minimise the data traffic through the network (i.e. with the data transmitted at step 203 in Figure 2).

The data set provides information necessary for the service provider system to set-up a communication channel with the third party server. Communication channels are defined and then exposed as a unique REST based service through a unique URI. A return URI can also be defined, which also provides a unique REST based service endpoint, available for the third party to post data to, and therefore back into the service provider system 101. The workflow is built using a proprietary building language, ZyncFlow. ZyncFlow exposes building blocks of ZyncFlow script to an end user; these blocks are sequentially dragged onto a "definition grid" which enables the user to define the following:

- A data form that is dynamically generated within an app on a mobile device enabling the user to use their mobile device as an input device for the workflow.
- Data capture fields. These fields are defined fields and capture necessary data from the user's device or account, or alternatively request the data to be manually entered by the user into the data form dynamically created
- Authentication of forms. All data must be checked to be valid.
- Definition of attached content, if required.
- Post-to point and definition of API service. This is the external third party provider's service API that can be consumed by the workflow as defined on the service provider system.
- Data actions. For example, update a database, format data, and/or exposure of data.
- Definition and dynamic creation of RESTful API end point that can be connected to, enabling content to be sent into the workflow from a third party.
- Definition of delivery of content to a specific mobile device. For example, defining the return content type as a warranty, document, or external link.

Once the workflow is set-up the service provider system 101 sends a request for a warranty to the third party server 104 using the defined API as specified in the workflow definition at step 304. The third party server is defined within the service provider system by an XML based Schema external to the service provider server 101 which was set up when the workflow was built as described above. In response, at step 305, the third party server returns the required warranty. A tracking key is used to ensure that the warranty being moved within the workflow relates to the specific merchant, the third party warranty provider and the end user.

When the service provider system 101 receives the warranty it then pre-populates the warranty with all of the required consumer data that it has stored in its memory. The merchant device 103 may then be sent a message requesting the unique identifier for the product, but this is preferably automatically included in the initial communication at step 303. The service provider server 101 then sends the warranty document to the user device 102. In order to reduce data traffic and in order to simplify the process for the user, the warranty is preferably sent to the user with the message for requesting approval of the payment or once the payment process has been completed along with the transaction completion authorisation code. The user is then able to fill in any information into the warranty that has not been autocompleted by the service provider system 101, and then approve the warranty at step 307. Again, it is preferable that the approval of the warranty is sent from the user device 101 to the service provider system 101 when the user approves the transaction. Between steps 306 and 307 the user could save the warranty and continue the completion of the warranty process at a later point in time. This might be preferable if the user is paying at a shop counter. A tracking code is used to check where the warranty is in terms of which step in the defined workflow, and to also enable data being sent back to the service provider to be injected into the correct workflow for the correct warranty.

When the service provider system 101 has received the completed and approved warranty, and confirmation of the payment being processed is received, a copy of the warranty certificate is sent to both the third party server 104 and the user device 102. The warranty can then be stored in the user device 102 by the mobile app, which allows the warranty to be easily accessed at any time. The warranty process is then complete.

Another application of the workflow functionality is delivery tracking. If a consumer purchases a product to be delivered, it is common for there to be information available for tracking such a product. When the consumer purchases a product to be delivered, a workflow with a third party delivery company can be set-up to "pull" tracking data into the workflow. Consequently, the consumer can then use their mobile device to track the delivery information without the need for the merchant to issue a tracking code to the consumer, or the consumer having to visit a 3rd party website to manually enter a tracking code and track their delivery. The tracking information is provided to the user within the service provider environment 100.

The same principles apply to a consumer wishing to have their goods made available to them for collection at a local store. The merchant's system connects back with the service provider system to indicate the store where the goods are to be picked up from and when the goods are available. The service provider system connects to the merchant's endpoints through the defined workflow and populates necessary data for that store to process. The consumer's mobile device can now locate the store where their goods are to be picked up from, and read any other attached data in the workflow. The merchant has not had to develop an internal workflow nor rely on the consumer speaking to staff to see when their goods are ready to be picked up. The consumer's mobile device now provides the main interaction point between the merchant and the consumer. The consumer uses their own mobile device to track data on their pick up.

The workflow functionality can also be used to enable a user device as an input device to capture data for market research using a survey or basic questionnaire. Hence, a business can create a "data form" and have it made available on the user's mobile device, e.g. after a purchase. The user may complete the form by providing the requested data. The completed form is then captured, along with user identifying and hardware specific data, all of which is then sent back into the defined workflow within the service provider system. A third party market research company may therefore be included in the process for collecting the results of the questionnaire. This process allows for better data capture of individuals completing questionnaires. In addition, the efficiency of the questionnaire completion process is improved. Furthermore, the security provisions provided by the service provider system mean that the requirement for secure communication certificates to be purchased and installed for secure questionnaires is not required.

User Interface

The user device is provided with a user interface known as the Pinboard. The Pinboard is a single user interface provided on the user device that allows for messages such as pushed messages used to deliver vouchers, loyalty scheme updates, and information on personalised deals to be displayed, without the user needing to go beyond the Pinboard section of the device. Other information that can be included in the Pinboard includes electronic receipts, warranties, travel documentation, and presentations, which may be sent to the user by the pushing services or workflow functionalities described above. Content can be delivered to the mobile device and stored locally through the communications channel (either pushed or pulled).

New content made available to the user is therefore delivered through a single efficient point, making the mobile device hardware more efficient at relaying tangible content to an end user. The user no longer needs to browse their device for different content that is available to them, rather the user is taken directly to that content from the Pinboard and provided with options to "claim" and/or store that content, where appropriate, within their virtual wallet, i.e. the user account with the service provider. Once claimed, the service provider system allocates the claimed content to a given user and registers it to a particular device. This process therefore removes the need for the device to remain connected to the service provider system as "claimed" content is now directly accessed from memory storage on the user's device. In addition, some Pinboard messages deliver a direct link to external content. When a Pinboard message is selected with an external link, the user can be taken directly to that external content. Finally, a user can be taken to a particular message within the app on the user device from the Pinboard itself. By selecting an individual cell, the user jumps into the service provider app on the user device at the correct place to see the content that was being displayed on that cell.

The Pinboard functionality and particularly the display characteristics shall now be described with reference to Figure 5, which shows a homepage screen 400 for the app installed on the user device 102.

The homepage screen comprises various items 402, 403, 404, 405 that link the user to different parts of the service provider app. For example, each of these items links the user to one of account information, purchase information, loyalty information, or any other part of the app. The user is therefore able to browse content via items 402,

403, 404 and 405. The pinboard icon 401 is also provided on the homepage of the app, which as has already been mentioned, provides a simple user interface that allows the user to quickly and easily view messages stored within the app.

Visually, the Pinboard is arranged as a celled or tiled screen that shows all of the latest messages to the user, informing them of Pinboard and associated content without the need for the user to access each and every message directly. The Pinboard can be defined with different cell strucutres, for example, the size of cells, the number of cell, and when in a two dimensional array, the shape of the array can be variable, as can how the cells interconnect. In Figure 5, six interconnecting cells are shown, but the number of cells differs in alternative arrangements. The cells are arranged in a rectangular grid structure.

In Figure 5, the Pinboard Icon cells are split vertically and horizontally. However, in alternative arrangements cells may even be split diagonally so that multiple content is displayed on the cells. The cells are arranged so that some messages can be displayed on a single cell, while other messages or content may be displayed on multiple cells. Multiple messages are therefore selected to be displayed on the cells of the Pinboard such that all of the cells are filled with information. For example, in Figure 5, three messages that are not related are displayed: a ticket is displayed across the top three cells, a voucher in the bottom left cell, and a loyalty point message in the bottom middle and bottom left cells. Providing multiple messages on the array of cells enables greater efficiency for a user to consume overview content at a glance.

The application operating the Pinboard groups new messages received by the user device 102 together based on their type and referenced content. For example, all new messages relating to vouchers are grouped together. These groups of messages are then ordered in terms of when they will be displayed on the Pinboard Icon cells. Complete groups are processed first, for example messages all containing vouchers are displayed, with each voucher being allocated a single cell that is animated and then locked with the other cells to deliver a single icon, displaying 3 vouchers. In some cases it is not possible to group messages in this way and also provide messages on all cells. Hence, in such circumstances a determination is made as to which content is to be displayed to fit on the available Pinboard cells. Figure 5 shows such circumstances.

Once the selected messages are displayed, the Pinboard icon remains static for a set period of time, before each cell unlocks and rotates to thereby display another cell. The Pinboard cells can rotate in opposite directions and independently of each other. When the cells re-lock together the next Pinboard message content overview is displayed to the user, either on a single cell or across multiple cells to form one larger icon / cell. New content at this point is allocated to each of the cells (complete group content again). This process is repeated so that the messages and content being displayed continually changes. In the case that no new content is received, the user's Pinboard messages that are stored in the devices memory are cycled through in the Pinboard display.

Certain content, for example a boarding pass on a flight, requires 3 cells to display sufficient detail to make the details of the boarding pass clear on the Pinboard. In such a case, the boarding pass is loaded only on the Pinboard when three cells are available together. Other messages, such as vouchers only need a single cell in order to provide sufficient detail to the user. Hence, the number of cells taken up by each message depends on the information in the message that needs to be displayed. In order to determine how many cells a message needs, each message is provided with a code indicative of a number of cells required by the message. This code is assigned according to the type of message, e.g. whether the message is a ticket or a voucher. The required number of cells for a type of message is determined based on an average amount of information that needs to be presented to a user to make the message intelligible to the user. In alternative arrangements, each message is analysed to determine key information to be displayed and the content of the Pinboard message is created and the number of cells required to display the content is assigned. The Pinboard message as displayed in the Pinboard icon is typically a "summary" of the full content. This is set-up when the Pinboard message was created. However, in some configurations and for some content, a summary is not provided, rather rules are applied to the message to determine the summary. For example, a voucher code and name is provided. Once the user selects a Pinboard message, they are taken to the full message (displayed full screen). Hence, the system is arranged to determine which messages are to be displayed by analysing the possible messages that could be displayed and determining which of those messages could fit within the cell structure to thereby maximise the usage of the cell structure.

While the above-exemplary embodiment of the invention relates to displaying content relating to a virtual wallet, it will be appreciated that the principles of the Pinboard are applicable for providing an efficient use of screen space for displaying any type of content to a user.

Intelligent Scaling

As has already been discussed, the service provider system is preferably implemented in a cloud environment, i.e. by one or more could-based servers. When implemented as a cloud-based system, the service provider system includes intelligent cloud resource scaling functionality in order to maximise efficiency of resource usage.

The intelligent cloud resource scaling functionality is arranged to monitor the server capacity used by the service provider system and adjust the size of the cloud resources used to support the service provider system according to the monitored usage. When demand for use of the service provider system is high, for example for financial transactions in the run up to Christmas in the UK, the system is able to obtain additional resource from the cloud. When resource is low, the system is able to shed resource from the cloud. This therefore maximises the efficiency of resource usage, reduces the cost associated with use of such resources and raises the energy efficiency of the physical datacentre.

In order to provide the intelligent cloud resource scaling functionality a monitoring system is required. The monitoring is provided locally to the relevant cloud-based servers. This is necessary because scaling may take place within a certain country or geographical region when shops close at the end of the day and demand for use of the service provider system substantially drops. Whereas in other countries or geographical regions shops may just be opening due to time differences. Local monitoring systems are deployed locally to a localised cloud data centre. For example, European servers may be located in Ireland and Amsterdam, while servers providing service to Canada and the USA may be situated in 2 locations across northern America. Hence, separate monitoring of these disparate servers is required. These monitoring services are connected to the cloud underlying operating system platform. In alternative arrangements, the local monitoring can be installed on a physical server located anywhere in the world.

The local monitoring system uses a scaling rules engine that uses the data captured by the system along with profile data obtained over a period of time to decide if new resources are required. The parameters monitored by the local monitoring system include one or more of:

- Database loads, i.e. the amount of activity on the service provider system
- Average web server request times. The local monitoring system issues basic web requests to the service provider system and monitors the length of time it takes to receive a response.
- Web latency.
- Current Date.
- Time of the day.
- Promotional offers, i.e. if a large or popular merchant has recently issued an offer that may mean that a large number of users may soon be using the service provider system.
- Content within the service provider system and its corresponding expiration date.

The system is able to vary, add or remove resources based on the current characteristics of the system as determined in accordance with the above characteristics. Alternatively, the system is able to perform a prediction as to what resources will be required in the future based on current information and past trends. It is preferable to predict expected resource requirements in order to attempt to ensure that there are sufficient resources in place to meet increased demand before demand forces the cloud resources to scale, which causes a lag period where the system will slow down as required resources are brought online. The frequency with which the cloud resources are varied will depend on the frequency at which the cloud provider allows for resources to be added and/or removed. Preferably, the resources are monitored to allow for the resources to be adjusted as near to constantly as is possible.

Two specific independent algorithms are used by the service provider in order to determine scalability requirements. The first focusses on the actual load of the service provider and allocates a numerical value based on the results obtained. This numerical value is checked against a tolerance number (an upper and lower value is configured based on that geographical location for that virtual cloud / server).

The second algorithm identifies anticipated loads and performance requirements on the service provider based on previous trends and analytics of data captured over a period of time. This result is allocated a numerical value and again, upper and lower tolerance values are read from configuration.

The two numerical values and tolerance values are then added to deliver a final numerical value and tolerance (lower and upper value). The numerical value is then checked against a system configuration value and measured against the tolerance value. If the final value exceeds the upper tolerance value, then additional resources are required. The amount of additional resources is determined by the difference in the tolerance value. If the required resources are below the lower tolerance value then resources may be removed by the system.

The various methods described above may be implemented by a computer program. The computer program may include computer code arranged to instruct a computer to perform the functions of one or more of the various methods described above. The computer program and/or the code for performing such methods may be provided to an apparatus, such as a computer, on a computer readable medium or computer program product. The computer readable medium could be, for example, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, or a propagation medium for data transmission, for example for downloading the code over the Internet. Alternatively, the computer readable medium could take the form of a physical computer readable medium such as semiconductor or solid state memory, magnetic tape, a removable computer diskette, a random access memory (RAM), a read-only memory (ROM), a rigid magnetic disc, and an optical disk, such as a CD-ROM, CD-R/W or DVD.

An apparatus such as a computer may be configured in accordance with such code to perform one or more processes in accordance with the various methods discussed herein. Such an apparatus may take the form of a computer system or data processing system. Such a data processing system may be a distributed system. For example, such a data processing system may be distributed across a network.

Claims:

1. A method for providing secure communication between a plurality of parties, the method comprising:

receiving, at an authorisation system, a first communication from a first party, the first communication comprising information identifying a second party to which the first communication is directed;

verifying, at the authorisation system, an identity of the first party;

sending, from the authorisation system when the identity of the first party is verified, a second communication to the second party in accordance with the first communication;

receiving, at the authorisation system, a third communication from the second party issued in response to the second communication; and

verifying an identity of the second party responsive to receipt of the third communication.

2. The method according to claim 1, wherein the method is for providing secure communication between a plurality of parties for processing a financial transaction between the plurality of parties.

3. The method according to claim 2, wherein:

the first party is a merchant and the first communication comprises information identifying the financial transaction to be processed; and

the second party is a consumer and the third communication comprises information indicating that the second party approves the financial transaction.

4. The method according to claim 3, further comprising processing the financial transaction when the authorisation system receives approval of the financial transaction from the second party and verifies the identity of the second party.

5. The method according to any one of claims 2 to 4, wherein if the identity of either the first or second party is not successfully verified then the financial transaction is cancelled.

6. The method according to any one of claims 3 to 5, wherein the first communication comprises information identifying the merchant and the method further comprises:

identifying if the consumer has a loyalty account with the merchant; and

sending, if the consumer has a loyalty account with the merchant, a fourth communication to the merchant comprising information identifying the consumer's loyalty account with the merchant and information identifying the financial transaction for the merchant to add loyalty points to the consumer's loyalty account with the merchant.

7. The method according to any preceding claim, further comprising determining, at the authorisation system, the identity of the second party from the information identifying the second party provided in the first communication.

8. The method according to any preceding claim, further comprising:

receiving location information indicative of a location of the second party; and

determining if the location information is indicative of fraudulent activity.

9. The method according to claim 8, further comprising:

receiving location information indicative of a location of the first party; wherein

determining if the location information is indicative of fraudulent activity comprises comparing the location information indicative of a location of the first party with the location information indicative of a location of the second party.

10. The method according to claim 8 wherein determining if the location information is indicative of fraudulent activity further comprises comparing the location information indicative of a location of the second party with information indicative of a previous location of the second party.

11. The method according to any preceding claim, further comprising

creating a profile of the second party, the profile indicative of characteristics of the second party;

determining current characteristics of the second party;

comparing the profile of the second party with the current characteristics of the second party; and

identifying the presence of fraudulent activity by the second party in accordance with the comparison of the profile.

12. The method according to claim 11, wherein the characteristics of the second party include location information associated with the second party.

13. The method according to claim 11 or claim 12, further comprising:

receiving, with the third communication, information indicative of the current characteristics of the second party.

14. The method according to any preceding claim, wherein the identity of the first and second parties is verified in accordance with information provided in the first and third communications respectively.

15. The method according to claim 14, wherein the information provided in the third communication is security information, wherein the identity of the second party is verified by comparing the security information received in the third communication with security information stored in a memory of the authorisation system.

16. The method according to claim 15, wherein the security information comprises information identifying a device being used by the third party and information identifying the third party using the device.

17. The method according to claim 16, wherein the information identifying a device used by the third party comprises one or more of:

information identifying hardware of the device;
information identifying the type of the device;
information identifying an operating system used by the device;
information identifying a version of the operating system of the device; and
a UDID or Unique ID of the device.

18. The method according to claim 16 or claim 17, wherein the information identifying the third party using the device comprises one or more of:

an OAuth identifier; and
a PIN code.

19. The method according to any one of claims 16 to 18, wherein the information identifying a device being used by the third party and information identifying the third party using the device is encrypted using an encryption process to form the security information.

20. The method according to claim 19, wherein an item of the information identifying the device being used by the third party or an item of information identifying the third party using the device is used as an encryption key for producing the encrypted fingerprint.

21. The method according to claim 9, wherein a PIN code associated with the third party is used as the encryption key.

22. The method according to any preceding claim, wherein verifying the identity of the first party comprises determining if the first party is registered with the authorisation system.

23. Apparatus for providing secure communication between a plurality of parties, the apparatus comprising:

a communication for communicating with a plurality of parties; and

a processor arranged to process information; wherein

the apparatus is arranged to perform the method of any preceding claim.

24. The apparatus according to claim 23, wherein the apparatus is a cloud-based server arrangement.

25. A computer readable medium comprising computer readable code operable, in use, to instruct a computer system to perform the method of any one of claims 1 to 22.

26. A method for verifying validity of communications, the method comprising:

receiving a communication from a device associated with a user, the communication comprising information identifying the device associated with the user and information for verifying an identity of the user associated with the device; and

determining if the device is a device registered for use by the user of the device; and

verifying if the user is the registered user of the device.

27. The method according to claim 26, further comprising:

performing further processing associated with the communication if the device is determined to be registered for use by the user of the device and the user is verified as the registered user of the device.

28. The method according to claim 27, wherein the communication comprises information identifying a second user to which the communication is directed, and wherein the further processing associated with the communication comprises sending a communication to the second user.

29. The method according to claim 28, wherein determining if the device is a device registered for use by the user of the device comprises comparing information identifying the device associated with the user with information identifying the device associated with the user stored in a memory of an authorisation system performing the verification.

30. The method according to claim 29, wherein the information identifying the device associated with the user comprises one or more of:

information identifying hardware of the device;
information identifying the type of the device;
information identifying an operating system used by the device;
information identifying a version of the operating system of the device; and
a UDID or Unique ID of the device.

31. The method according to any one of claims 28 to 30, wherein determining if the user is the registered user of the device comprises comparing information for verifying an identity of the user associated with the device with information for verifying an identifying of the user associated with the device stored in a memory of an authorisation system performing the verification.

32. The method according to claim 31, wherein the information for verifying an identity of the user associated with the device comprises one or more of:

an OAuth identifier; and
a PIN code.

33. The method according to any one of claims 29 to 31, wherein the information identifying the device associated with the user and information for verifying an

identifying of the user associated with the device is received as an encrypted fingerprint providing an individual identifier of the user at the user device.

34. The method according to claim 33, wherein an item of the information identifying the device associated with the user or an item of information for verifying an identifying of the user associated with the device is used as an encryption key for producing the encrypted fingerprint.

35. The method according to claim 34, wherein a PIN code associated with the user is used as the encryption key.

36. The method according to any one of claims 26 to 35, wherein the method is for verifying the validity of communications for use in processing of financial transactions.

37. Apparatus for verifying validity of communications, the apparatus comprising:
a communication unit for communicating with a plurality of parties; and
a processor arranged to process information; wherein
the apparatus is arranged to perform the method of any one of claims 26 to 36.

38. The apparatus according to claim 37, wherein the apparatus is a cloud-based server arrangement.

39. A computer readable medium comprising computer readable code operable, in use, to instruct a computer system to perform the method of any one of claims 26 to 36.

40. A method for producing security information to be associated with a communication, the security information for verifying the validity of the communication, the method comprising:
obtaining information identifying a device associated with a user and information for verifying an identity of the user associated with the device; and
producing security information in accordance with the information identifying a device associated with a user and information for verifying an identity of the user associated with the device.

41. The method according to claim 40, further comprising:

encapsulating the security information in a communication to be sent by the user device.

42. The method according to claim 41, wherein the security information is encapsulated within a header of the communication.

43. The method according to any one of claims 40 to 42 wherein the information identifying the device associated with the user comprises one or more of:

information identifying hardware of the device;

information identifying the type of the device;

information identifying an operating system used by the device;

information identifying a version of the operating system of the device; and

a UDID or Unique ID of the device.

44. The method according to any one of claims 40 to 43, wherein the information for verifying an identity of the user associated with the device comprises one or more of:

an OAuth identifier; and

a PIN code.

45. The method according to any one of claims 40 to 44, wherein the security information is produced by encrypting the information identifying the device associated with the user and the information for verifying an identity of the user associated with the device.

46. The method according to claim 45, wherein an item of the information identifying the device associated with the user or an item of information for verifying an identity of the user associated with the device is used as an encryption key for producing the encrypted security information.

47. The method according to claim 46, wherein a PIN code associated with the user is used as the encryption key.

48. The method according to any one of claims 40 to 47, wherein the security information is fingerprint.

49. Apparatus for producing security information to be associated with a communication, the security information for verifying the validity of the communication, the apparatus comprising:

a processor arranged to perform the method of any one of claims 40 to 48.

50. The apparatus according to claim 49, wherein the apparatus is a smart phone.

51. A computer readable medium comprising computer readable code operable, in use, to instruct a computer system to perform the method of any one of claims 40 to 48.

52. A method for preparing a packet for secure and efficient transmittal over a network, the method comprising:

inserting content to be transmitted over a network within a body of a packet; and

inserting security information for authentication purposes within a header of the packet.

53. The method according to claim 52, wherein the security information is produced according to any one of claims 40 to 48.

54. The method according to claim 52 or claim 53, further comprising transmitting the packet to a recipient.

55. Apparatus for preparing a packet for secure and efficient transmittal over a network, the apparatus comprising a processor arranged to perform the method of any one of claims 52 to 55.

56. A computer readable medium comprising computer readable code operable, in use, to instruct a computer system to perform the method of any one of claims 52 to 55.

57. A method for verifying the validity of information received over a network, the method comprising:

receiving, over a network, a packet comprising content within a body of the packet and security information for authentication purposes within a header of the packet;

obtaining, from the header of the packet, the security information; and

verifying the received packet in accordance with the security information.

58. The method according to claim 57, wherein the verification is performed according to any one of claims 26 to 36, wherein the packet of claim 57 is the communication of any one of claims 26 to 36, and the security information of claim 57 is the information identifying the device associated with the user and the information for verifying an identity of the user associated with the device of any one of 26 to 36.

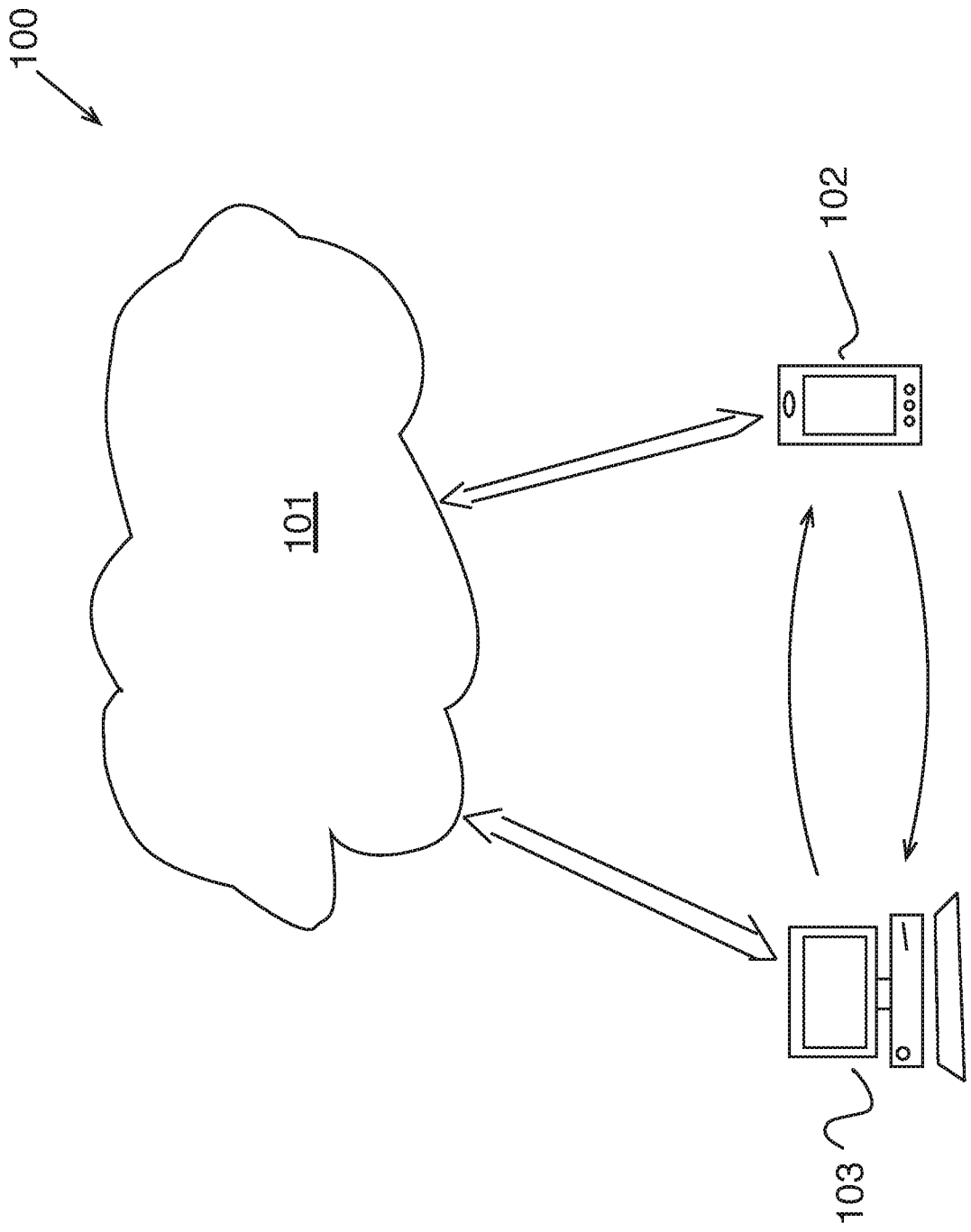


Figure 1

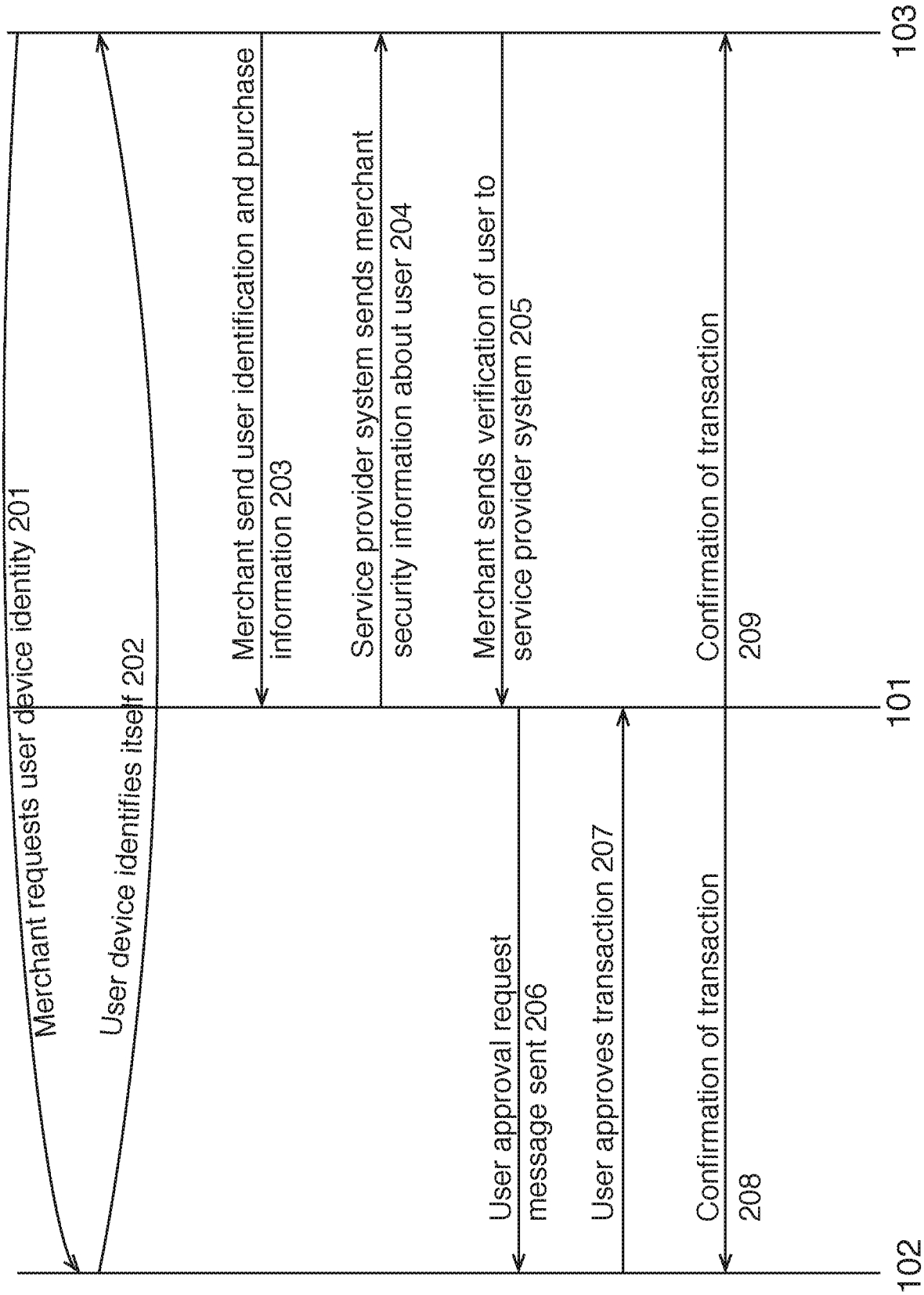

Merchant requests user device identity 201
User device identifies itself 202
Merchant send user identification and purchase information 203
Service provider system sends merchant security information about user 204
Merchant sends verification of user to service provider system 205
User approval request message sent 206
User approves transaction 207
Confirmation of transaction 208
Confirmation of transaction 209
101
102
103

Figure 2

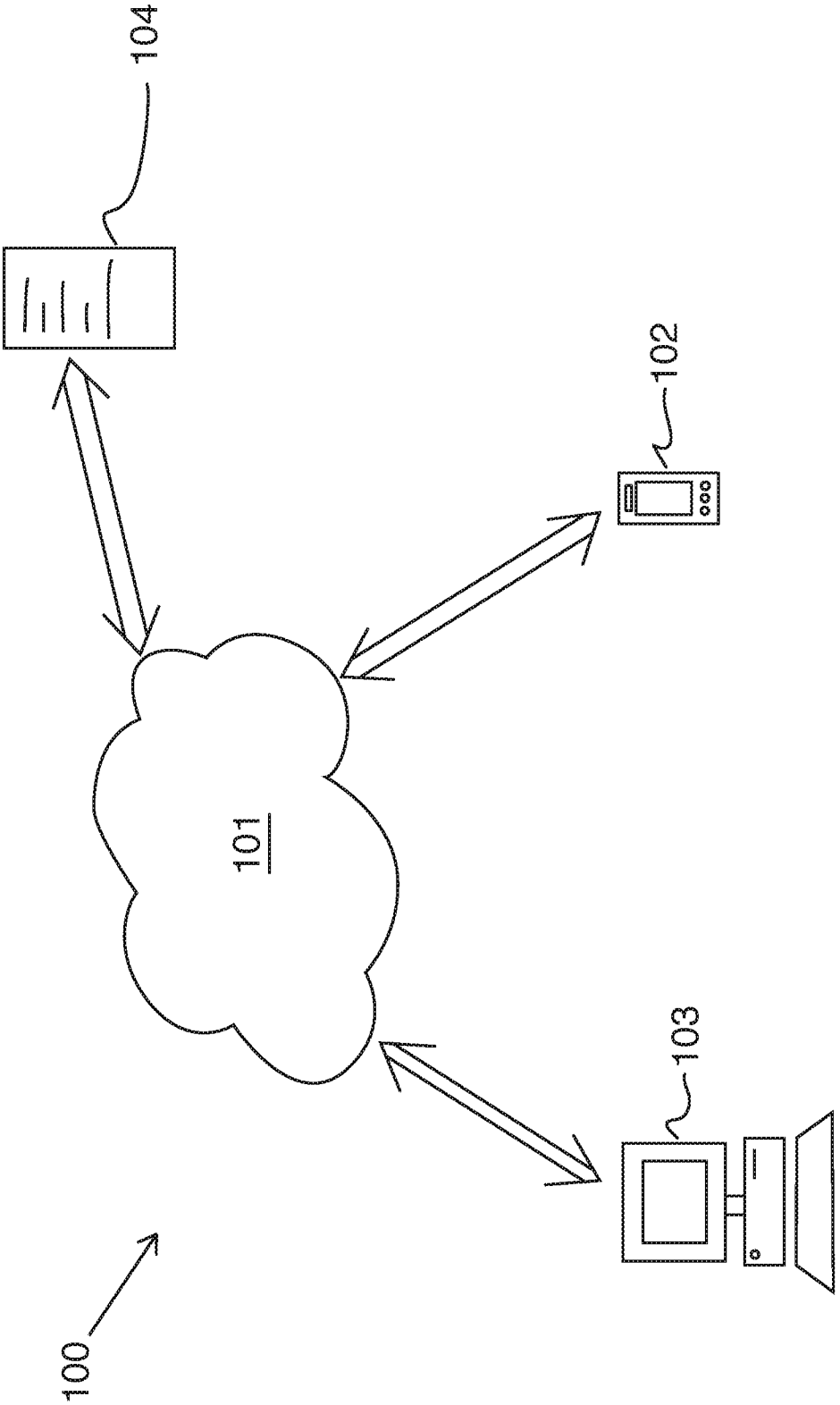


Figure 3

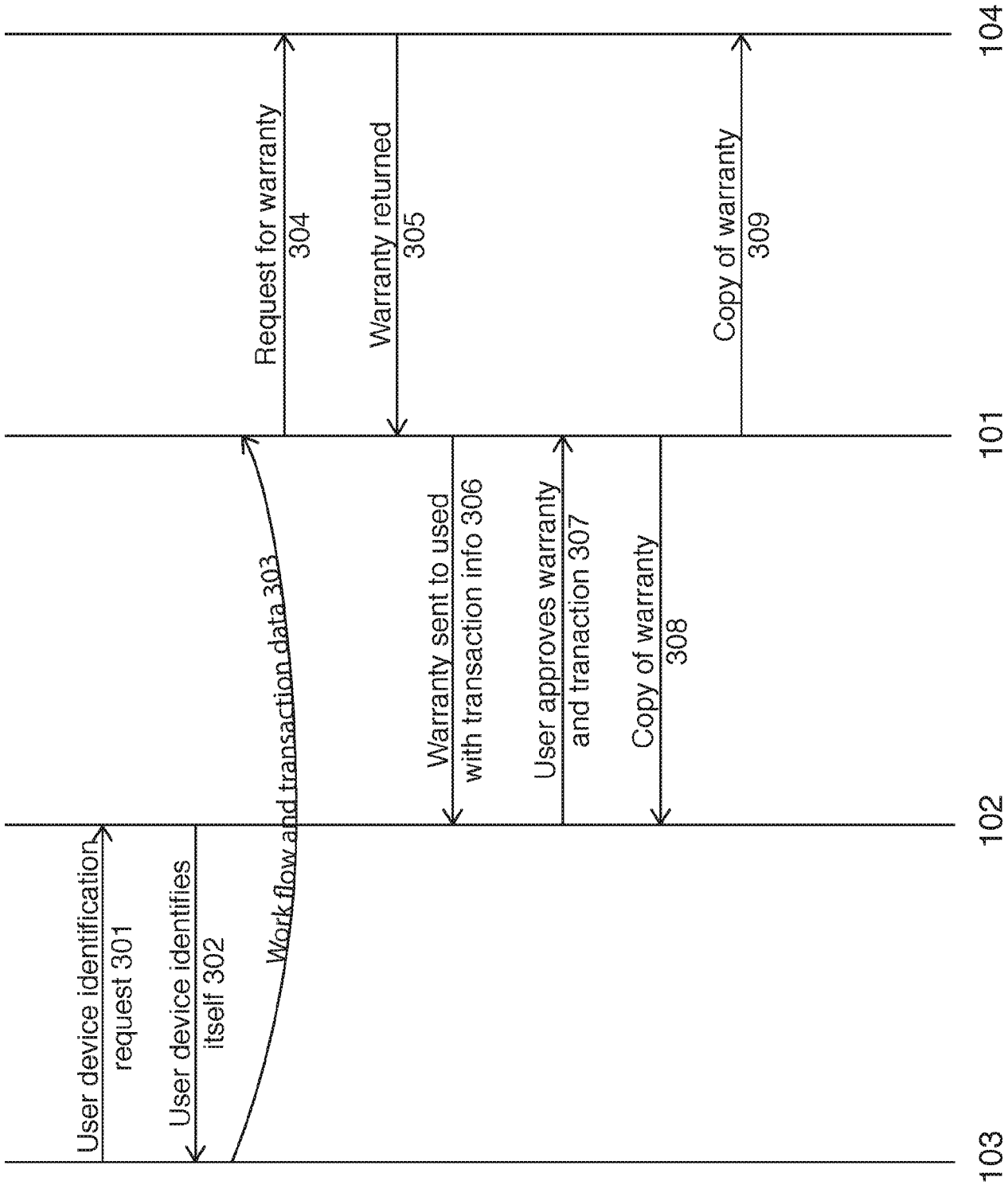

User device identification request 301
User device identifies itself 302
Work flow and transaction data 303
Request for warranty 304
Warranty returned 305
Warranty sent to used with transaction info 306
User approves warranty and tranaction 307
Copy of warranty 308
Copy of warranty 309
103
102
101
104

Figure 4

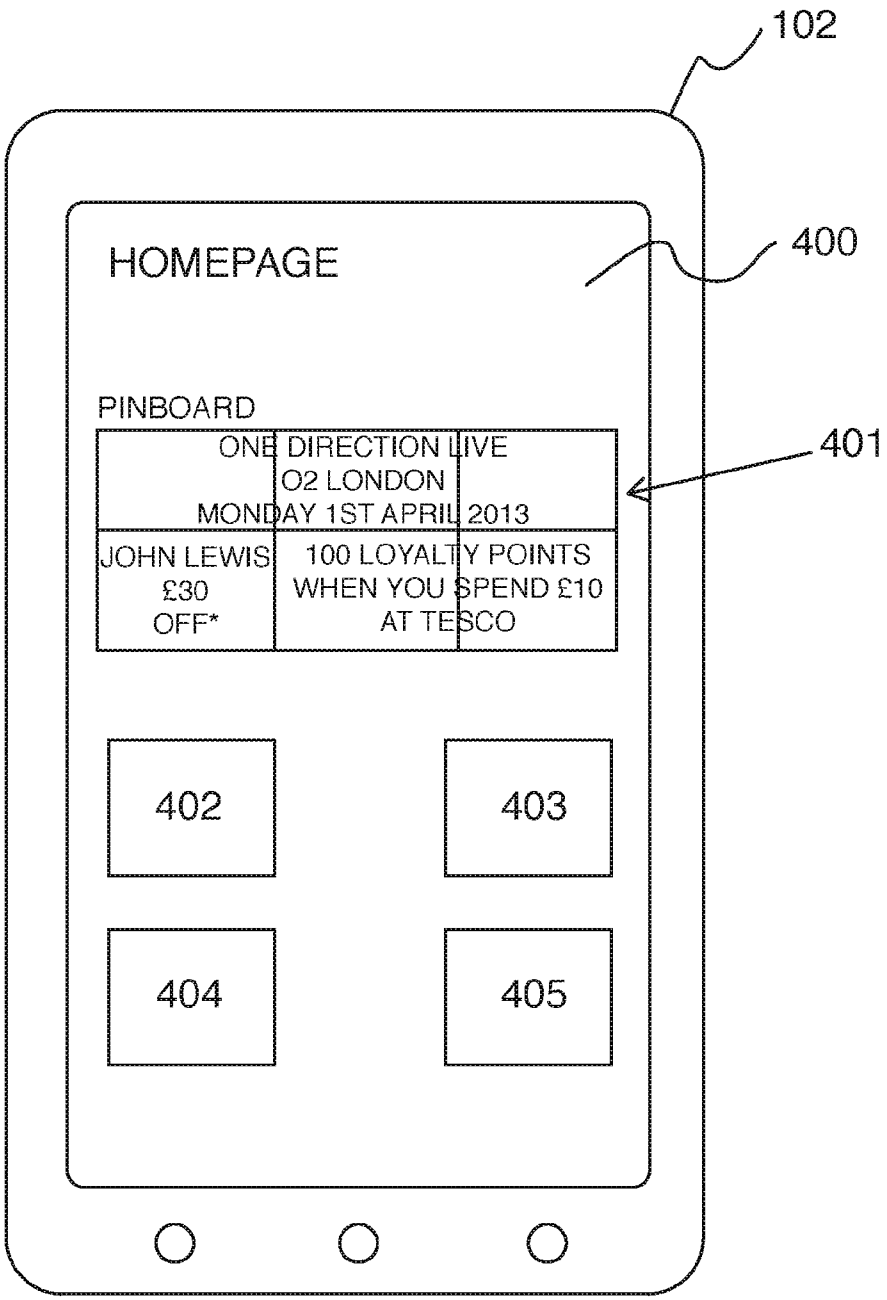

102
HOMEPAGE
400
PINBOARD
401
ONE DIRECTION LIVE
O2 LONDON
MONDAY 1ST APRIL 2013
JOHN LEWIS
£30
OFF*
100 LOYALTY POINTS
WHEN YOU SPEND £10
AT TESCO
402
403
404
405

Figure 5