



(51) International Patent Classification:
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)
G06Q 20/10 (2012.01)

(21) International Application Number:
 PCT/CA2017/051451

(22) International Filing Date:
 01 December 2017 (01.12.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
 62/428,659 01 December 2016 (01.12.2016) US
 62/546,107 16 August 2017 (16.08.2017) US

(71) Applicant: ROYAL BANK OF CANADA [CA/CA]; 6th Floor, North Wing, 1 Place Ville Marie, Montreal, Québec H3C 3A9 (CA).

(72) Inventors: LAU, Alex Tak Kwun; c/o 6th Floor, North Wing, 1 Place Ville Marie, Montreal, Québec H3C 3A9 (CA). ORTIZ, Edison U.; c/o 12001 Research Pkwy, Suite 432, Orlando, Florida 32822 (US). GUPTA, Akhil; c/o 6th Floor, North Wing, 1 Place Ville Marie, Montreal, Québec H3C 3A9 (CA). SHARMA, Mohit; c/o 6th Floor, North Wing, 1 Place Ville Marie, Montreal, Québec H3C 3A9 (CA). MANUEL, Lucas Joseph; c/o 6th Floor, North Wing, 1 Place Ville Marie, Montreal, Québec H3C 3A9 (CA). SU, Tian Jou Tendency; c/o 6th Floor, North Wing, 1 Place Ville Marie, Montreal, Québec H3C 3A9 (CA).

(54) Title: SYSTEM AND METHOD FOR MESSAGE RECIPIENT VERIFICATION

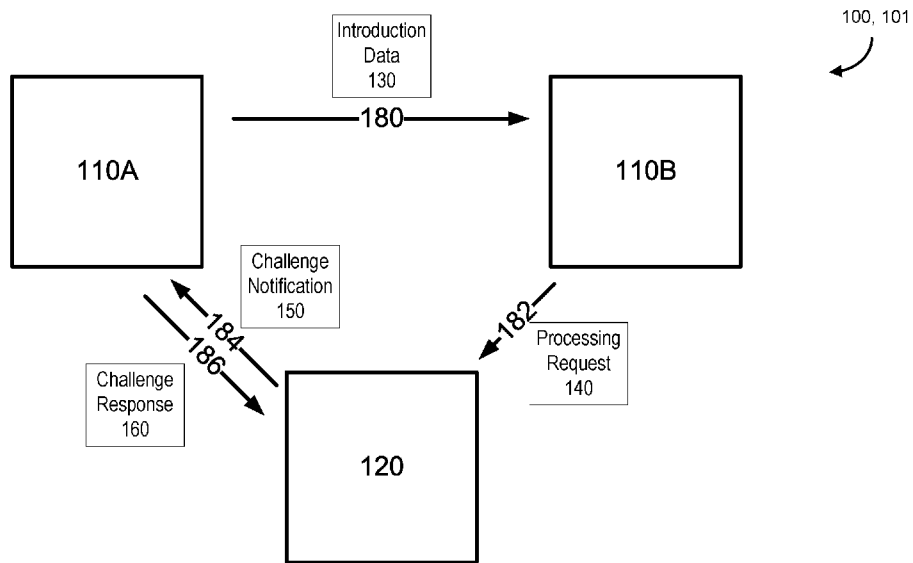


FIG. 1

(57) Abstract: An electronic device includes a communication interface and at least one processor configured for: transmitting to or receiving from a second electronic device over proximity-based communication channel an introduction message including a first encryption key; receiving, from a server via the at least one communication interface, a challenge notification providing notification of a challenge to be completed to initiate a data process, the challenge notification including or providing access to at least one data field associated with a verification challenge; identifying, from the at least one data field, an encrypted challenge response value; decrypting the encrypted challenge response value with a key corresponding to the first encryption key; and transmitting the decrypted challenge response value to the server to complete the challenge to initiate the data process.



(74) **Agent: NORTON ROSE FULBRIGHT CANADA LLP;**
1 Place Ville Marie, Suite 2500, Montreal, Québec H3B 1R1
(CA).

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

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

Published:

- with international search report (*Art. 21(3)*)
- in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE

SYSTEM AND METHOD FOR MESSAGE RECIPIENT VERIFICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present disclosure claims all benefit including priority to United States Provisional Patent Application 62/428,659, filed December 1, 2016, and entitled "SYSTEM AND METHOD FOR MESSAGE RECIPIENT VERIFICATION"; and to United States
5 Provisional Patent Application 62/546107, filed August 16, 2017, and entitled "SYSTEM AND METHOD FOR MANAGEMENT OF POINT-TO-POINT TRANSACTIONAL DATA MESSAGES". The entireties of these provisional applications are hereby incorporated by reference.

10 FIELD

[0002] Embodiments of the present disclosure generally relate to the field of electronic message processing, and more specifically, embodiments relate to electronic message processing requiring identity verification.

BACKGROUND

15 [0003] Messaging applications often rely on a central identity provider to verify the authenticity of a sender and a recipient of a message. For example, in messaging or social networking applications, users often sign into an authenticated session with their credentials to verify their identities.

[0004] It is however not always the case that a central identity provider exists for a
20 particular application. For example, INTERAC™ email money transfer (IEMT) enables money movement between any parties as long as the recipients have access to an email address. In order to accept the IEMT, the recipient is required to answer a challenge question which is created by the sender.

[0005] To be effective, the sender must come up with a challenge question that the
25 recipient would know the answer to, but could not be easily guessed or ascertained by a third party who may intercept the email.

SUMMARY

[0006] In some embodiments, aspects of the present disclosure may reduce the risk associated with a challenge process required in a multi-party data process initiation.

5 [0007] In accordance with one aspect, there is provided an electronic device. The electronic device includes at least one communication interface; at least one memory; and at least one processor configured for: transmitting to or receiving from a second electronic device over proximity-based communication channel an introduction message including a first encryption key; receiving, from a server via the at least one communication interface, a challenge notification providing notification of a challenge to be completed to initiate a data
10 process, the challenge notification including or providing access to at least one data field associated with a verification challenge; identifying, from the at least one data field, an encrypted challenge response value; decrypting the encrypted challenge response value with a key corresponding to the first encryption key; and transmitting the decrypted challenge response value to the server to complete the challenge to initiate the data process.

15 [0008] In accordance with another aspect, there is provided a method for multi-party initiation of a data process. The method includes: at a first electronic device, transmitting to or receiving from a second electronic device over proximity-based communication channel an introduction message including a first encryption key; receiving, from a server via at least one communication interface, a challenge notification providing notification of a challenge to
20 be completed to initiate a data process, the challenge notification including or providing access to at least one data field associated with a verification challenge; identifying, from the at least one data field, an encrypted challenge response value; decrypting the encrypted challenge response value with a key corresponding to the first encryption key; and transmitting the decrypted challenge response value to the server to complete the challenge
25 to initiate the data process.

[0009] In accordance with another aspect, there is provided an electronic device, comprising: at least one communication interface; at least one memory; and at least one processor configured for: transmitting to or receiving from a second electronic device over proximity-based communication channel an introduction message including a first encryption

key; generating a challenge response value and encrypting the challenge response value with a key corresponding to the first encryption key; and transmitting a processing request to a server, the processing request including a plurality of data fields including: the challenge response value in a challenge response field, and the encrypted response value in at least one other field of the plurality of fields; wherein the processing request requests initiation of a data process at the server when a verification challenge presented to the second electronic device is completed, the verification challenge including the at least one other field.

[0010] In accordance with another aspect, there is provided a method for multi-party initiation of a data process, the method comprising: at a first electronic device, transmitting to or receiving from a second electronic device over proximity-based communication channel an introduction message including a first encryption key; generating a challenge response value and encrypting the challenge response value with a key corresponding to the first encryption key; and transmitting a processing request to a server, the processing request including a plurality of data fields including: the challenge response value in a challenge response field, and the encrypted response value in at least one other field of the plurality of fields; wherein the processing request requests initiation of a data process at the server when a verification challenge presented to the second electronic device is completed, the verification challenge including the at least one other field.

DESCRIPTION OF THE FIGURES

[0011] In the figures, embodiments are illustrated by way of example. It is to be expressly understood that the description and figures are only for the purpose of illustration and as an aid to understanding.

[0012] Embodiments will now be described, by way of example only, with reference to the attached figures, wherein in the figures:

[0013] FIG. 1 is a schematic diagram showing aspects of an example system and data flow.

[0014] FIG. 2 is a schematic diagram showing aspects of another example system and data flow.

[0015] FIG. 3 is a schematic diagram of computing device, exemplary of an embodiment.

[0016] FIG. 4 is schematic diagram showing aspects of an example system and data flow.

[0017] FIG. 5 is schematic diagram showing aspects of another example system and data flow.

5 [0018] FIG. 6 is an example user interface including a code for communicating introduction data.

[0019] FIG. 7 is schematic diagram showing aspects of another example system and data flow.

[0020] FIG. 8 shows an example payment processing data flow.

10 [0021] FIG. 9 shows another example payment processing data flow.

DETAILED DESCRIPTION

[0022] In some applications, such as a payment processing application, a trusted server sits between a sender device and a recipient device. However, to increase compatibility, the trusted server may not act as an identity provider which validates the authenticity of the sender and the recipient.

15

[0023] In some systems, such as the INTERAC™ email money transfer (IEMT) system, communication with a central server can occur via an unsecure channel such as email. For example, in IEMT, a sender device only has to provide an email address of the recipient with which the IEMT server initiates communication with the recipient. However, email is an inherently unsecure communication mechanism which can be subject to interception, eavesdropping, impersonation, etc.

20

[0024] In order to authenticate the recipient, the server may receive one or more input fields from the sender device. For example, the server may receive one or more messages from the sender device including data in a challenge question field and a challenge answer field. In order to be effective, the sender must create a challenge which only the recipient would be able to answer. This verification process can be weak if the challenge inputted by

25

the sender is based on information that would be easy to guess or that a third party may be able to ascertain. “What is your birthday?”, “What is my middle name?”, and “What is my dog’s name?” are examples of information which may be discovered by a third party through a social media website or otherwise. In another example, the sender may verbally tell the recipient the answer to the inputted challenge in person or over the phone. In some instances, this verbal communicate may be eavesdropped by a third party.

[0025] While strong challenge questions can be a somewhat effective authentication mechanism, in some instances, the creation and answering of a challenge question may be a burden. In situations where the sender is with the recipient and can visually confirm the recipient’s identify, the challenge-answer mechanism may be redundant.

[0026] In some instances, aspects of the example embodiments illustrated herein may simplify the authentication process when the sender and the recipient are within proximity of each other. In some embodiments, a simplified process may operate with an existing central server with little or no modification to the server.

[0027] In some instances, aspects of the example embodiments illustrated herein may improve the security of the authentication process. In some embodiments, the improvement in security may be realized with little or no modification to existing central servers.

[0028] FIG. 1 shows aspects of an example system 100 and data flow 101 between devices in the system. The system 100 includes a device 110A associated with a recipient, a device 110B associated with a sender, and a server 120. In an example situation, the sender and the recipient devices are in close proximity to each other. For example, a sender and a recipient may be having dinner together and the sender may want to reimburse a recipient for paying the bill.

[0029] At 180, the recipient’s device 110A sends introduction data 130 to the sender’s device 110B. In some embodiments, this transmission is done through a proximity based communication mechanism. For example, in one embodiment, the recipient device displays, on a display device, an image such as a QR code or barcode which encodes introduction data 130. In some embodiments, the displayed image is captured by an imaging or other

scanning device at the sender's device 110B, which can be decoded to obtain the introduction data 130.

[0030] In some embodiments, the introduction data 130 can be sent through near field communication (NFC), radio-frequency identification (RFID), or any other proximity based communications. Communication over these mechanisms can be described as being a communication over a proximity-based communication channel.

[0031] In some embodiments, a proximity-based communication channel can involve any communication mechanism which requires a line of sight between the communicating devices. In some situations, the proximity-based communication mechanism may require for the two communicating devices to touch or to be in visual range of each other, which may enable a user to visually confirm the identity of the user of the other device.

[0032] In some embodiments, the device may require a user to authorize the transmission of the introduction data by inputting credentials once the user has made visual confirmation of the other user's identity. In some embodiments, this can include entering a password or providing biometric information to the device such as a fingerprint or facial scan. In some embodiments, upon receipt of the credentials, the device transmits the introduction message.

[0033] In some embodiments, the introduction data 130 can be sent through other communication mechanisms such as Bluetooth™, WiFi, SMS, and the like; however, in some instances, these approaches may be less secure. In some embodiments, QR codes, NFC or other proximity communication mechanisms may be used to initiate a pairing of the two devices 110A, 110B (e.g. Bluetooth™ pairing) which may, in some instances, improve the security of the transmission and/or reduce the likelihood of third party eavesdropping or interception.

[0034] In some embodiments, the introduction data 130 includes receiver identification data and an encryption key. In some embodiments, the receiver identification data includes an email address or other information required for the server 120 to identify and/or communicate with the receiver device 110A or an account associated with the receiver /

receiver device 110A. For example, if the server requires an email address or user ID to contact the account associated with the receiver or receiver device 110A, this information can be included in the receiver identification data. In some examples, the receiver identification data can include a phone number associated with the receiver device, an
5 account number or other identifier, a username or any other identifier(s) associated with the receiver device or a receiver account.

[0035] In some embodiments, the introduction data 130 includes an encryption key. The encryption key can, in some embodiments be an asymmetric key. For example, the encryption key communicated in the introduction data can be a public key that is part of a
10 public-private key pair. The private key can be stored on the recipient device 110A.

[0036] In some embodiments, the new keys can be generated periodically, or each time introduction data is to be transmitted to a sender device 110B.

[0037] In some embodiments, the encryption key can be a symmetric key. However, in some instances, this may be less secure than an asymmetric key.

15 [0038] In some embodiments, the introduction data can include transaction information such as a payment amount.

[0039] Upon receipt of the introduction data, in some embodiments, the sender device 110B is configured to generate a processing request 140 for initiating a process with the server 120, such as an IEMT. The generated processing request 140 may include a number
20 of fields such as a recipient identifier field (e.g. email address), payor data field(s) (e.g. information for identifying and authorizing access to a payment account, a payment amount, etc.), a challenge field, and a challenge answer field. In some embodiments, the fields may include a memo field and/or any other optional information field. The number, format and type of fields in the initiation request may be defined by a protocol or service provided by the
25 server 120.

[0040] In some embodiments, one or more processors on the sender device generate the payment data fields based on the introduction data and/or data inputted by the sender at the sender device. For example, the sender may input a payment amount or other data on a

keypad, touchscreen, or other input device. In some embodiments, the payee info may be based on data from the introduction data received from the recipient device 110A or data inputted at the sender device 110B.

5 [0041] In some embodiments, the processor(s) on the sender device 110B generate data for security answer field. In some embodiments, the security answer may be generated by a random number generator. In some embodiments, the security answer may be generated from an input from the sender, for example by hashing or encoding a text or other input received at the sender device.

10 [0042] In some embodiment, the generated security answer may be a random or pseudo-random string of text or other characters. In some instances, the random nature of the security answer is more difficult to guess by a third party than a recognizable word or numerical security answer provided by the sender.

15 [0043] In some embodiments, the processor(s) on the sender device 110B generate data for communicating the security answer to the recipient in one or more of the data fields sent 182 to the server with the processing request 140. In some embodiments, the number, type, length, and/or arrangement of the data fields must meet the requirements of the application/process/service running on the server.

20 [0044] In some embodiments, the sender device processor(s) encrypt the security answer with the security key provided in the introduction data. The encrypted security answer is then sent with the processing request in any field which is ultimately sent to the recipient device 110A as part of the challenge notification. For example, the encrypted security answer can be sent in a challenge question field, a memo field, a description field, or any other non-functional field. In some embodiments, the processor(s) repurpose one or more of these fields (which are intended to store other data) to store the encrypted security answer.

25 [0045] In some embodiments, the encrypted security answer may be split across multiple fields. For example, if an encrypted security answer is too long to fit in the challenge question field, a portion of the encrypted security answer may be sent in the encrypted security answer field and a portion of the encrypted security answer may be sent in a memo

field. In some instances, utilizing multiple defined fields to send an encrypted security answer may allow for longer answers which may improve the security of the process. In some instances, the arrangement of the encrypted security answer across the multiple fields may further obfuscate the security answer.

5 [0046] The server 120 processes the processing request 140 which may include accessing payment servers and accounts, verifying/authenticating payor information, processing funds, and/or any other actions required for the server 120 to process the request. In some embodiments, the server 120 may operate in its traditional manner with its traditional request data fields, and may be unaware of the aspects of the authentication
10 process occurring between the sender and recipient devices outside of the server process.

[0047] In some instances, embodiments of the methods and systems described herein may operate without requiring any modification or control of the server 120.

[0048] The server 120 sends a challenge notification 150 to the recipient device 110A. In some embodiments, the challenge notification 150 includes a number of data fields such as
15 a challenge question field, memo fields, description fields, and/or any other field. Some or all of the data in these fields may be obtained from the sender device 110B in the processing request 140. In some embodiments, each field containing a portion of the encrypted challenge answer is included in the challenge notification 150.

[0049] In some embodiments, the challenge notification provides access to the challenge
20 notification data fields. For example, in some embodiments, the challenge notification message may include a link, URL, credentials or otherwise provide access to a web page, server or data service which presents or transmits the data fields to the recipient device.

[0050] In some embodiments, the challenge notification may be an email message, an SMS, or any other messaging service or protocol. For example, an IEMT challenge
25 notification may be an email to a recipient email address which includes payor information, payment data fields, as well as a challenge question and memo/description fields.

[0051] In some embodiments, a process operating on the recipient device 110A is configured to recognize and to begin processing the challenge notification. In some

embodiments, the recipient device 110A does not need to display and/or request challenge question information to a user. The recipient device 110A may optionally display a portion of the notification including payor information, payment amount, and/or any other field that does not contain the encrypted security answer.

5 [0052] In some embodiments, the recipient device 110A may display a confirmation user interface for requesting and receiving a confirmation input indicating that the recipient accepts the process/transaction identified in the challenge notification. In some embodiments, the recipient device 110A may automatically process the challenge notification without receiving any input or confirmation from the user. In some such
10 embodiments, confirmations and display of process/transaction details may occur before the transmission of the introduction message.

[0053] The recipient device 110A obtains the encrypted security answer from the challenge notification fields, and decrypts the security answer using the encryption key stored at the recipient device 110A (e.g. private key in a private-public key pair, or the
15 symmetric key).

[0054] In some embodiments, the recipient device 110A identifies the encrypted challenge response value (security answer) from one or more data fields provided by the challenge notification.

[0055] In some embodiments, processors at the recipient device 110A combine values
20 from two or more of the data fields to obtain the encrypted challenge response value. In some embodiments, combining the values can include concatenating the two or more values from different data fields into a single value. In other embodiments, other logical or mathematical operations can be performed to combine the values.

[0056] At 186, the recipient device 110A sends a challenge response 160 including the
25 security answer (decrypted challenge response) to the server 120 to complete the challenge and initiate a data process. In some embodiments, initiating the data process can include initiating the process to transfer funds from an account associated with the recipient to the account associated with the sender.

[0057] In some embodiments, the system may be utilized for other data processes such as secure file sharing. In some such embodiments, upon successful completion of the challenge, the server may present or enable access to one or more files to the recipient device.

5 [0058] In other embodiments, the system, devices and methods described herein may be applied to initiate any other suitable data process involving verification or input from multiple parties.

[0059] In some instances, the automatic generation of security questions and answers, and the automatic processing of the challenge notification and response can simplify and/or
10 speed up the process between the sender and the recipient while still maintaining the security of an authenticated transaction via visual recognition and confirmation of the sender/recipient and/or the proximity of the devices.

[0060] If an asymmetric key pair is used in the process, only the recipient device 110A which holds the private key is able to decrypt the security answer, so any third party who
15 may intercept the challenge notification will not be able to guess or otherwise answer the challenge question.

[0061] In some embodiments, the introduction message can include an identifier for associating the data process. For example, the recipient device 110A can be configured to generate a unique identifier for associated with the data process to be initiated by the server,
20 and storing this unique identifier in association with an encryption key corresponding to the key sent with the introduction message. The sender device 110B will include the unique identifier in the processing request to the server, and the server includes the unique identifier with the challenge notification data fields. In this manner, the recipient device 110A is able to identify the correct key for decrypting the encrypted response value by accessing the stored
25 key associated with the identifier.

[0062] FIG. 2 shows aspects of another example system 200 and data flow 201 between devices in the system. Similar to FIG. 1, the system 100 includes a device 110A associated with a recipient, a device 110B associated with a sender, and a server 120.

[0063] The example system 200 in FIG. 2 includes an authentication server 205. In some embodiments, before a recipient device 110A sends introduction data 130 to a sender device 110B, the recipient device 110A sends the encryption key and/or the sender identifier to the authentication server 205 to be signed. In some embodiments, the recipient device or
5 a recipient account must be registered and authenticated with the authentication server. The authentication server 205 digitally signs the encryption key and/or the sender identifier to the recipient device 110A which sends the signed encryption key and/or the sender identifier in the introduction data 130. In some embodiments, a signature for the encryption key and/or the sender identifier can hashing and/or encoding the encryption key and/or the sender
10 identifier with a key at the authentication server 205.

[0064] Upon receipt of the signed encryption key and/or sender identifier, at 281, before sending the processing request 140, the sender device 110B verifies the signature of the encryption key and/or sender identifier with the authentication server.

[0065] In some instances, this may improve the verification of the authenticity of the receiver device, and/or may provide some control over which devices may utilize the system
15 200.

[0066] In some embodiments, the operations of the receiver device and/or the sender device may be provided for and/or controlled by an application operating on the respective devices. For example, a mobile wallet application running on each device may provide for
20 the generation, communication and/or processing of the introduction message 130, the processing request 140, the challenge notification 150 and/or the challenge response 160.

[0067] In some embodiments, the recipient device 110A may send a data field to the sender device 110B in the introduction data or otherwise which indicates an application, version and/or capability of the recipient device 110A to automatically process the challenge
25 notification from the server 120.

[0068] In some embodiments, the sender device 110B may include a defined string or other indicator in one of the challenge question, memo or other fields. The defined string or other indicator can, in some instances, be used to indicate that the challenge notification can

be automatically processed by decrypting the answer in one of the fields. Upon receipt of a challenge notification including the defined identifier, a process running on the receiver's device can recognize the challenge notification as a notification that can be automatically processed.

5 [0069] In some embodiments, additional decoding data may be included in one of the fields provided by the sender device and included in the challenge notification. In some examples, the additional decoding data may indicate a decrypting scheme, a location of the encrypted answer, and/or any other information or parameter for identifying and/or decrypting the encrypted answer.

10 [0070] In some embodiments, a sender and recipient may verify each other's identities even when they are not in close proximity to each other. For example, a sender and recipient may be communicating over a video call. In some embodiments, the introduction data 130 can be communicated from the recipient device 110A to the sender device 110B by the recipient presenting the QR code on the recipient device 110A up to the video call camera,
15 which can be captured by the sender device 110B from a display showing the video call.

[0071] In the examples in FIGS. 1 and 2, the introduction message is transmitted from the recipient device 110A to the sender device 110B. However, in other embodiments, the introduction message including the first encryption key can be transmitted from the sender device 110B to the recipient device 110A.

20 [0072] In conjunction with the systems described herein or otherwise, FIG. 4 shows aspects of an example data flow diagram including interactions with an Interac e-Transfer™ server.

[0073] At 41, a requester device receives one or more inputs including an amount which is being requested to be transferred to an account associated with the requester device. In
25 some embodiments, the input can be received from an input device such as a keypad, touchscreen, audio microphone or any other suitable input device. In some embodiments, the input can be received from an application or process operating on the requester device. For example, the input can be received from a payment application, an intelligent personal

assistant (e.g. Apple Inc.'s Siri™ or Google Assistant™), a mobile wallet, a messaging application, a banking application or the like.

[0074] In some embodiments, the requester device generates a public/private key pair for use in the introduction information. In some embodiments, data fields corresponding to a requester profile are obtained from a payment application, an address book database, a user profile or otherwise. In some embodiments, some of this information may be selected from a list or received via an input device.

[0075] At 42, introduction data is send to the payer device. In FIG. 4, the introduction data is illustrated as being encoded in a QR code for communication to the payer device. In some embodiments, the introduction data include a payment amount, a requester name or other identifier, a requester phone number or e-mail address, the public key generated by the requester device, and/or any other fields which may be used by the Interac server.

[0076] At 43, the payer device receives the introduction data. In some embodiments, the payer device is configured to receive an input selecting an account associated with the payer device. In some embodiments, the account may be selected automatically from a payer profile. In some embodiments, upon receiving the introduction data, the payer device is configured to request a confirmation input to confirm that a user associated with the payer device authorizes the payment.

[0077] Upon receipt of such authorization, the payer device is configured to generate a security answer. The payer device encrypts the security answer with the public key for use in the security question.

[0078] At 44, the payer device sends an Interac e-transfer request to the Interac server. In some embodiments, the request includes a requester (destination) account identifier, a requestor email address or phone number, a payer (source) account identifier, a payment amount, and a security question which includes the encrypted security answer.

[0079] When the request is processed by the Interac server, the Interac server sends a challenge notification via an SMS or email to the requester device.

[0080] In some embodiments, the requester device is configured to execute an SMS or an e-mail listener application or process. In some embodiments, the listener application or process automatically detects messages including the challenge notification. In some embodiments, the requester device automatically select a default account for depositing the payment, optionally logs in to the account if required, and decrypts the security answer from the security question using the private key stored at the requester device.

[0081] In some embodiments, some of these steps may not be automatic and may require input from the user. For example, the device may require confirmation that the user wishes to receive the transfer, the device may require that the user input credentials to log into a financial institution account/application, and/or the device may require that the user select a financial institution and/or account rather than relying on a default value stored in a user profile or application.

[0082] Upon providing the security answer and selecting the account, the payment is handled by the Interac server.

[0083] In some instances, this system/process may provide for a simplified yet secure method for interacting with an existing payment infrastructure.

[0084] In conjunction with the systems described herein or otherwise, FIG. 5 shows aspects of an example data flow diagram including interactions with an electronic funds transfer server.

[0085] At 51, a requester device receives one or more inputs including an amount which is being requested to be transferred to an account associated with the requester device. In some embodiments, the input can be received from an input device such as a keypad, touchscreen, audio microphone or any other suitable input device. In some embodiments, the input can be received from an application or process operating on the requester device. For example, the input can be received from a payment application, an intelligent personal assistant (e.g. Apple Inc.'s Siri™ or Google Assistant™), a mobile wallet, a messaging application, a banking application or the like.

[0086] In some embodiments, introduction data fields corresponding to a requester name/nickname/identifier, a requester name and/or other fields used in an electronic funds transfer (such as 3PP) are obtained from a payment application, an address book database, a user profile or otherwise. In some embodiments, some of this information may be selected
5 from a list or received via an input device.

[0087] At 52, introduction data is send to the payer device. In FIG. 5, the introduction data is illustrated as being encoded in a QR code for communication to the payer device. In some embodiments, the introduction data include a payment amount, a requester name/nickname or other identifier, a requester account number or other account identifier, and/or any other
10 fields which may be used by the 3PP server.

[0088] At 53, the payer device receives the introduction data. In some embodiments, the payer device is configured to receive an input selecting an account associated with the payer device. In some embodiments, the account may be selected automatically from a payer profile. In some embodiments, upon receiving the introduction data, the payer device is
15 configured to request a confirmation input to confirm that a user associated with the payer device authorizes the payment. In some embodiments, the requestor account number or other account identifier may be obfuscated, partially masked or otherwise not displayed to the user at the payer device.

[0089] At 54, the payer device sends a 3PP e-transfer request to the Interac server. In
20 some embodiments, the request includes a requester (destination) account identifier, and a payer (source) account identifier, a payment amount.

[0090] At 55, the request and transfer of funds is processed by the 3PP server. At 56, the 3PP server sends a notification to the requester and/or payer device indicated the transfer was successful. In some instances, this system/process may provide for a simplified yet
25 secure method for interacting with an existing payment infrastructure.

[0091] In conjunction with the systems described herein or otherwise, FIG. 6 shows aspects of an example user interface. In some embodiment such a user interface may be generated by a web server for an online retailer. The user interface includes a QR code for

providing introduction information to a customer/payer device. Aspects of an example data flow which makes use of the introduction information on a website is shown in FIG. 7.

[0092] At 71, the requester device (i.e. web server or an associated requester device or process) obtains one or more inputs including an amount which is being requested to be transferred to an account associated with the requester device. In some embodiments, the input can be received or generated by the web server or an associated online commerce server. For example, the amount may be a total purchase amount for an online transaction (e.g. the total purchase amount of \$54 as illustrated in the example user interface in FIG. 6).

[0093] In some embodiments, the requester device sends the amount value and optionally any other introduction data values to a QR code API server. The QR code API server generates a QR code using the amount value and other optional values, and provides the QR code for display on the website.

[0094] In other embodiments, the requester device may run a local API or otherwise generate a QR code with an API server.

[0095] In some embodiments, data fields corresponding to a requester profile are automatically sent by the requester device to be encoded in the QR code. In some embodiments, the API server may automatically select the data fields to be encoded by matching the requester with a database of requesters available to the API server.

[0096] At 72, introduction data is received by the payer device by scanning the QR code. In some embodiments, the introduction data include a payment amount, a requester name or other identifier, a requester phone number or e-mail address, the public key generated by the requester device, and/or any other fields which may be used by the Interac server. In some embodiments, the introduction data includes a unique payment ID.

[0097] In some embodiments, the encryption key and encoded answer in a challenge question field mechanism as described above may be applied.

[0098] At 73, the payer device receives the introduction data. In some embodiments, the payer device is configured to receive an input selecting an account associated with the payer

device. In some embodiments, the account may be selected automatically from a payer profile. In some embodiments, upon receiving the introduction data, the payer device is configured to request a confirmation input to confirm that a user associated with the payer device authorizes the payment.

5 [0099] Upon receipt of such authorization, the payer device is configured to generate a security answer. The payer device encrypts the security answer with the public key for use in the security question.

[00100] At 74, the payer device sends an Interac e-transfer request to the Interac server. In some embodiments, the request includes a requester (destination) account identifier, a
10 requestor email address or phone number, a payer (source) account identifier, a payment amount, and the unique payment ID.

[00101] At 75, the payment request is processed as described in the other examples herein or otherwise.

[00102] In some situations, the online payment system may enable small businesses that
15 use personal rather than commercial accounts to receive online payments.

[00103] In some embodiments, the online payment system can work with existing payment infrastructure such as Interac and can be agnostic as to the financial institution server that is being used.

[00104] In some embodiments, the online payment system can be set to auto-deposit such
20 that transferred funds are automatically deposited without requiring receipt of a manually-inputted confirmation.

[00105] In some embodiments, the auto deposit system will identify a destination account based on an email ID. In some embodiments, aspects of the auto deposit system may allow for the traditional question-answer security to be removed from the process.

25 [00106] Aspects of the system, processes and architectures described herein may be applied to the traditional merchant-acquirer-credit card processor system illustrated in FIG. 8.

[00107] For example, as illustrated in FIG. 9, a financial institution server can be positioned between the merchant system and the acquirer system.

[00108] In some embodiments, the financial institution server can be configured to handle acquiring and settlement for client accounts associated with the financial institution. In some
5 embodiments, the financial institution can take on the risk of defaults while the acquirer can provide the technical infrastructure. In some embodiments, the acquirer cost may be lower as the risk is taken on by the financial institution. In some situations, the financial institution may be better suited to handle the risk as the accounts are known to the financial institution through their personal accounts.

10 [00109] In some embodiments, the financial institution can approve new accounts faster (instantly). In some embodiments, NFC tap on phone technology can be used which in some instances may be more secure. This may, in some situations, result in lower fees.

[00110] In some situations NFC tap ability can be provided via an application that is installed at a requester device and will not require physical hardware such as a point-of-sale
15 terminal to be sent to a new merchant.

[00111] FIG. 3 is a schematic diagram of computing device 110, exemplary of an embodiment. As depicted, computing device 110 includes at least one processor 302, memory 304, at least one I/O interface 306, and at least one network interface 308.

[00112] Each processor 302 may be, for example, any type of general-purpose
20 microprocessor or microcontroller, a digital signal processing (DSP) processor, an integrated circuit, a field programmable gate array (FPGA), a reconfigurable processor, a programmable read-only memory (PROM), or any combination thereof.

[00113] Memory 304 may include a suitable combination of any type of computer memory that is located either internally or externally such as, for example, random-access memory
25 (RAM), read-only memory (ROM), compact disc read-only memory (CDROM), electro-optical memory, magneto-optical memory, Ferroelectric RAM (FRAM), etc.

[00114] Each I/O interface 306 enables computing device 110 to interconnect with one or more input devices, such as a keyboard, mouse, camera, touch screen and a microphone, or with one or more output devices such as a display screen and a speaker.

5 [00115] Each network interface 308 enables computing device 110 to communicate with other components, to exchange data with other components, to access and connect to network resources, to serve applications, and perform other computing applications by connecting to a network (or multiple networks) capable of carrying data including the Internet, Ethernet, plain old telephone service (POTS) line, public switch telephone network (PSTN), integrated services digital network (ISDN), digital subscriber line (DSL), coaxial
10 cable, fiber optics, satellite, mobile, wireless (e.g. Wi-Fi, WIMAX), SS7 signaling network, fixed line, local area network, wide area network, and others, including any combination of these.

[00116] Computing device 110 is operable to register and authenticate users (using a login, unique identifier, and password for example) prior to providing access to applications,
15 a local network, network resources, other networks and network security devices. Computing devices may serve one user or multiple users.

[00117] The embodiments of the devices, systems and methods described herein may be implemented in a combination of both hardware and software. These embodiments may be implemented on programmable computers, each computer including at least one processor,
20 a data storage system (including volatile memory or non-volatile memory or other data storage elements or a combination thereof), and at least one communication interface.

[00118] Program code is applied to input data to perform the functions described herein and to generate output information. The output information is applied to one or more output devices. In some embodiments, the communication interface may be a network
25 communication interface. In embodiments in which elements may be combined, the communication interface may be a software communication interface, such as those for inter-process communication. In still other embodiments, there may be a combination of communication interfaces implemented as hardware, software, and combination thereof.

[00119] Throughout the foregoing discussion, numerous references will be made regarding servers, services, interfaces, portals, platforms, or other systems formed from computing devices. It should be appreciated that the use of such terms is deemed to represent one or more computing devices having at least one processor configured to execute software instructions stored on a computer readable tangible, non-transitory medium. For example, a server can include one or more computers operating as a web server, database server, or other type of computer server in a manner to fulfill described roles, responsibilities, or functions.

[00120] The technical solution of embodiments may be in the form of a software product. The software product may be stored in a non-volatile or non-transitory storage medium, which can be a compact disk read-only memory (CD-ROM), a USB flash disk, or a removable hard disk. The software product includes a number of instructions that enable a computer device (personal computer, server, or network device) to execute the methods provided by the embodiments.

[00121] The embodiments described herein are implemented by physical computer hardware, including computing devices, servers, receivers, transmitters, processors, memory, displays, and networks. The embodiments described herein provide useful physical machines and particularly configured computer hardware arrangements. The embodiments described herein are directed to electronic machines and methods implemented by electronic machines adapted for processing and transforming electromagnetic signals which represent various types of information.

[00122] The embodiments described herein pervasively and integrally relate to machines, and their uses; and the embodiments described herein have no meaning or practical applicability outside their use with computer hardware, machines, and various hardware components. Substituting the physical hardware particularly configured to implement various acts for non-physical hardware, using mental steps for example, may substantially affect the way the embodiments work. Such computer hardware limitations are clearly essential elements of the embodiments described herein, and they cannot be omitted or substituted for mental means without having a material effect on the operation and structure of the embodiments described herein. The computer hardware is essential to implement the

various embodiments described herein and is not merely used to perform steps expeditiously and in an efficient manner.

[00123] Although the embodiments have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein.

- 5 [00124] Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure, processes, machines, manufacture, compositions
10 substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized.

[00125] As can be understood, the examples described above and illustrated are intended to be exemplary only.

WHAT IS CLAIMED IS:

1. An electronic device, comprising:
 - at least one communication interface;
 - at least one memory; and
 - at least one processor configured for:
 - transmitting to or receiving from a second electronic device over proximity-based communication channel an introduction message including a first encryption key;
 - receiving, from a server via the at least one communication interface, a challenge notification providing notification of a challenge to be completed to initiate a data process, the challenge notification including or providing access to at least one data field associated with a verification challenge;
 - identifying, from the at least one data field, an encrypted challenge response value;
 - decrypting the encrypted challenge response value with a key corresponding to the first encryption key; and
 - transmitting the decrypted challenge response value to the server to complete the challenge to initiate the data process.
2. The electronic device of claim 1, wherein the first encryption key is a first key of an asymmetric encryption key pair, and the key corresponding to the first encryption key is a second key of the asymmetric encryption key pair; or
 - wherein the first encryption key is the same as the key corresponding to the first encryption key.
3. The electronic device of claim 1, wherein the proximity-based communication channel is at least one of a near-field communication channel, a radio-frequency identification channel, or a Bluetooth™ channel.
4. The electronic device of claim 1, wherein the proximity-based communication channel involves:
 - displaying an image including encoded introduction message data for scanning by the second electronic device; or

scanning the image including the encoded introduction message data displayed by the second electronic device.

5. The electronic device of claim 1, wherein the at least one processor is configured for transmitting the introduction message to the second electronic device; and wherein the introduction message includes: challenger identification data comprising a destination identifier or address for the server to communicate with the electronic device.

6. The electronic device of claim 1, wherein the at least one processor is configured for:

transmitting the introduction message to the second electronic device, the introduction message including a first identifier for associating with the data process; storing the first identifier in conjunction with the key corresponding to the first encryption key; and

upon receipt of the challenge notification including or providing access to the at least one data field including a data process identifier, identifying the key corresponding to the first encryption key for decrypting the encrypted challenge response value when the data process identifier matches the first identifier.

7. The electronic device of claim 1, wherein the challenge notification includes or provides access to a plurality of data fields; and wherein identifying the encrypted challenge response value comprises combining values from at least two of the plurality of data fields.

8. The electronic device of claim 1, wherein the data process electronically transfers funds from an account associated with the second electronic device to an account associated with the electronic device.

9. The electronic device of claim 1, wherein the proximity-based communication channel involves: displaying, over a video call, an image including encoded introduction message data for scanning by the second electronic device.

10. A method for multi-party initiation of a data process, the method comprising:

at a first electronic device, transmitting to or receiving from a second electronic device over proximity-based communication channel an introduction message including a first encryption key;

receiving, from a server via at least one communication interface, a challenge notification providing notification of a challenge to be completed to initiate a data process, the challenge notification including or providing access to at least one data field associated with a verification challenge;

identifying, from the at least one data field, an encrypted challenge response value;

decrypting the encrypted challenge response value with a key corresponding to the first encryption key; and

transmitting the decrypted challenge response value to the server to complete the challenge to initiate the data process.

11. The method of claim 10, wherein the first encryption key is a first key of an asymmetric encryption key pair, and the key corresponding to the first encryption key is a second key of the asymmetric encryption key pair; or

wherein the first encryption key is the same as the key corresponding to the first encryption key.

12. The method of claim 10, wherein the proximity-based communication channel is at least one of a near-field communication channel, a radio-frequency identification channel, or a Bluetooth™ channel.

13. The method of claim 10, wherein the proximity-based communication channel involves:

displaying an image including encoded introduction message data for scanning by the second electronic device; or

scanning the image including the encoded introduction message data displayed by the second electronic device.

14. The method of claim 10, comprising transmitting the introduction message to the second electronic device; and wherein the introduction message includes: challenger

identification data comprising a destination identifier or address for the server to communicate with the electronic device.

15. The method of claim 10, comprising:
transmitting the introduction message to the second electronic device, the introduction message including a first identifier for associating with the data process;
storing the first identifier in conjunction with the key corresponding to the first encryption key; and
upon receipt of the challenge notification including or providing access to the at least one data field including a data process identifier, identifying the key corresponding to the first encryption key for decrypting the encrypted challenge response value when the data process identifier matches the first identifier.
16. The method of claim 10, wherein the challenge notification includes or provides access to a plurality of data fields; and wherein identifying the encrypted challenge response value comprises combining values from at least two of the plurality of data fields.
17. The method of claim 10, wherein the data process electronically transfers funds from an account associated with the second electronic device to an account associated with the electronic device.
18. The method of claim 10, wherein the proximity-based communication channel involves: displaying, over a video call, an image including encoded introduction message data for scanning by the second electronic device.
19. A non-transitory, computer-readable medium or media having stored thereon computer-readable instructions which when executed configured at least one processor of a first electronic device for:
transmitting to or receiving from a second electronic device over proximity-based communication channel an introduction message including a first encryption key;
receiving, from a server via the at least one communication interface, a challenge notification providing notification of a challenge to be completed to initiate

a data process, the challenge notification including or providing access to at least one data field associated with a verification challenge;

identifying, from the at least one data field, an encrypted challenge response value;

decrypting the encrypted challenge response value with a key corresponding to the first encryption key; and

transmitting the decrypted challenge response value to the server to complete the challenge to initiate the data process.

20. An electronic device, comprising:

at least one communication interface;

at least one memory; and

at least one processor configured for:

transmitting to or receiving from a second electronic device over proximity-based communication channel an introduction message including a first encryption key;

generating a challenge response value and encrypting the challenge response value with a key corresponding to the first encryption key; and

transmitting a processing request to a server, the processing request including a plurality of data fields including: the challenge response value in a challenge response field, and the encrypted response value in at least one other field of the plurality of fields;

wherein the processing request requests initiation of a data process at the server when a verification challenge presented to the second electronic device is completed, the verification challenge including the at least one other field.

21. The electronic device of claim 20, wherein the first encryption key is a first key of an asymmetric encryption key pair, and the key corresponding to the first encryption key is a second key of the asymmetric encryption key pair; or

wherein the first encryption key is the same as the key corresponding to the first encryption key.

22. The electronic device of claim 20, wherein the proximity-based communication channel is at least one of a near-field communication channel, a radio-frequency identification channel, or a Bluetooth™ channel.

23. The electronic device of claim 20, wherein the proximity-based communication channel involves:

displaying an image including encoded introduction message data for scanning by the second electronic device; or

scanning the image including the encoded introduction message data displayed by the second electronic device.

24. The electronic device of claim 20, wherein the at least one processor is configured for receiving the introduction message from the second electronic device; and wherein the introduction message includes: challenger identification data comprising a destination identifier or address for the server to communicate with the second electronic device.

25. The electronic device of claim 20, wherein the at least one processor is configured for:

receiving the introduction message from the second electronic device, the introduction message including a first identifier for associating with the data process;

transmitting to the server the first identifier in one of the plurality of data fields of the processing request for inclusion in the presentation of the verification challenge.

26. The electronic device of claim 20, wherein the at least one processor is configured for splitting the encrypted response value into at least two portions and transmitting the at least two portions to the server in at least two data fields of the processing request.

27. The electronic device of claim 20, wherein the data process electronically transfers funds from an account associated with the electronic device to an account associated with the second electronic device.

28. The electronic device of claim 20, wherein the proximity-based communication channel involves: scanning by the electronic device an image captured from a video call, the image including encoded introduction message data.
29. A method for multi-party initiation of a data process, the method comprising:
at a first electronic device, transmitting to or receiving from a second electronic device over proximity-based communication channel an introduction message including a first encryption key;
generating a challenge response value and encrypting the challenge response value with a key corresponding to the first encryption key; and
transmitting a processing request to a server, the processing request including a plurality of data fields including: the challenge response value in a challenge response field, and the encrypted response value in at least one other field of the plurality of fields;
wherein the processing request requests initiation of a data process at the server when a verification challenge presented to the second electronic device is completed, the verification challenge including the at least one other field.
30. The method of claim 29, wherein the first encryption key is a first key of an asymmetric encryption key pair, and the key corresponding to the first encryption key is a second key of the asymmetric encryption key pair; or
wherein the first encryption key is the same as the key corresponding to the first encryption key.
31. The method of claim 29, wherein the proximity-based communication channel is at least one of a near-field communication channel, a radio-frequency identification channel, or a Bluetooth™ channel.
32. The method of claim 29, wherein the proximity-based communication channel involves:
displaying an image including encoded introduction message data for scanning by the second electronic device; or

scanning the image including the encoded introduction message data displayed by the second electronic device.

33. The method of claim 29, comprising: receiving the introduction message from the second electronic device; and wherein the introduction message includes: challenger identification data comprising a destination identifier or address for the server to communicate with the second electronic device.

34. The method of claim 29, comprising:
receiving the introduction message from the second electronic device, the introduction message including a first identifier for associating with the data process;
transmitting to the server the first identifier in one of the plurality of data fields of the processing request for inclusion in the presentation of the verification challenge.

35. The method of claim 29, comprising splitting the encrypted response value into at least two portions and transmitting the at least two portions to the server in at least two data fields of the processing request.

36. The method of claim 29, wherein the data process electronically transfers funds from an account associated with the electronic device to an account associated with the second electronic device.

37. The method of claim 29, wherein the proximity-based communication channel involves: scanning by the electronic device an image captured from a video call, the image including encoded introduction message data.

38. A non-transitory, computer-readable medium or media having stored thereon computer-readable instructions which when executed configured at least one processor of a first electronic device for:

transmitting to or receiving from a second electronic device over proximity-based communication channel an introduction message including a first encryption key;

generating a challenge response value and encrypting the challenge response value with a key corresponding to the first encryption key; and transmitting a processing request to a server, the processing request including a plurality of data fields including: the challenge response value in a challenge response field, and the encrypted response value in at least one other field of the plurality of fields;

wherein the processing request requests initiation of a data process at the server when a verification challenge presented to the second electronic device is completed, the verification challenge including the at least one other field.

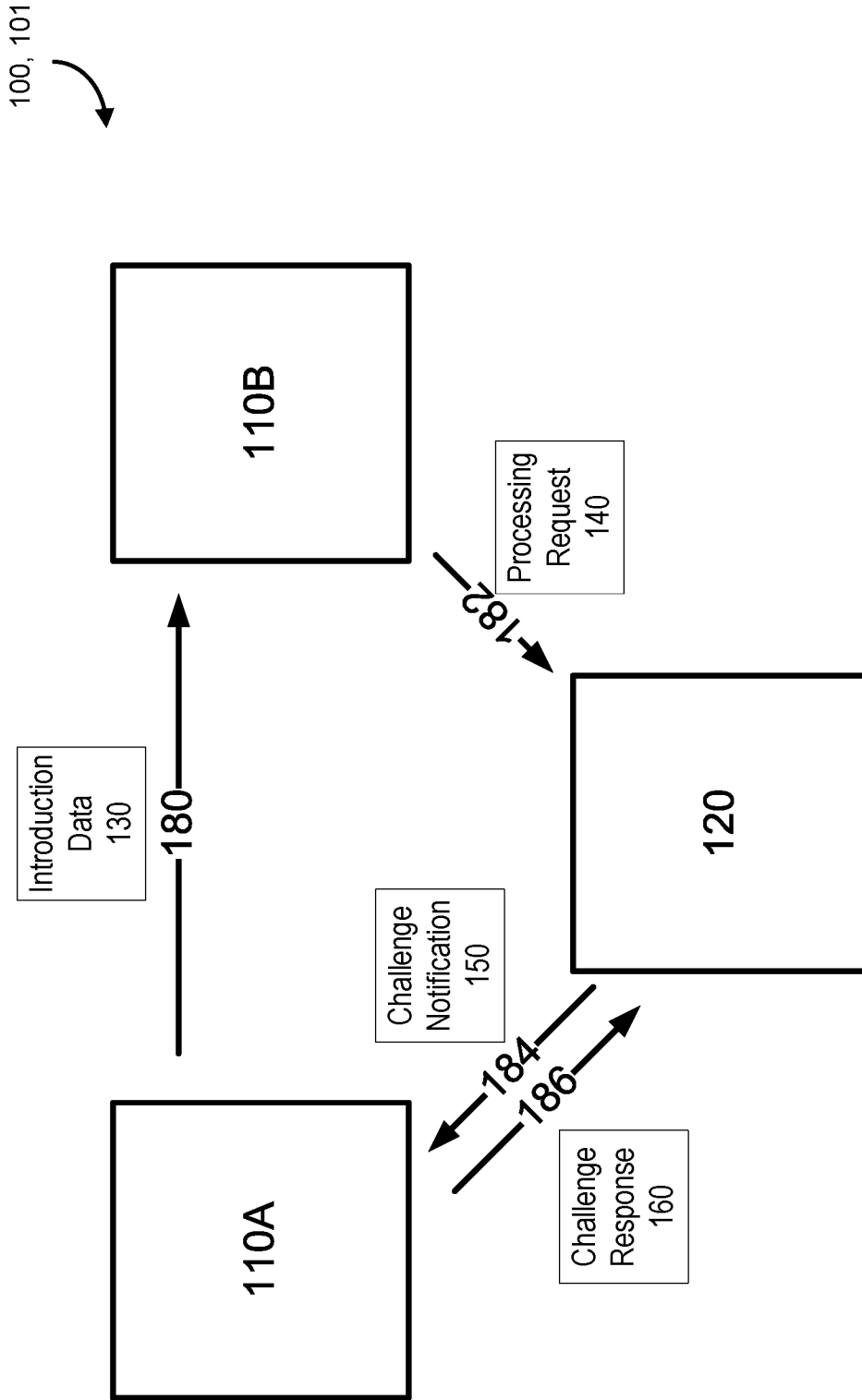


FIG. 1

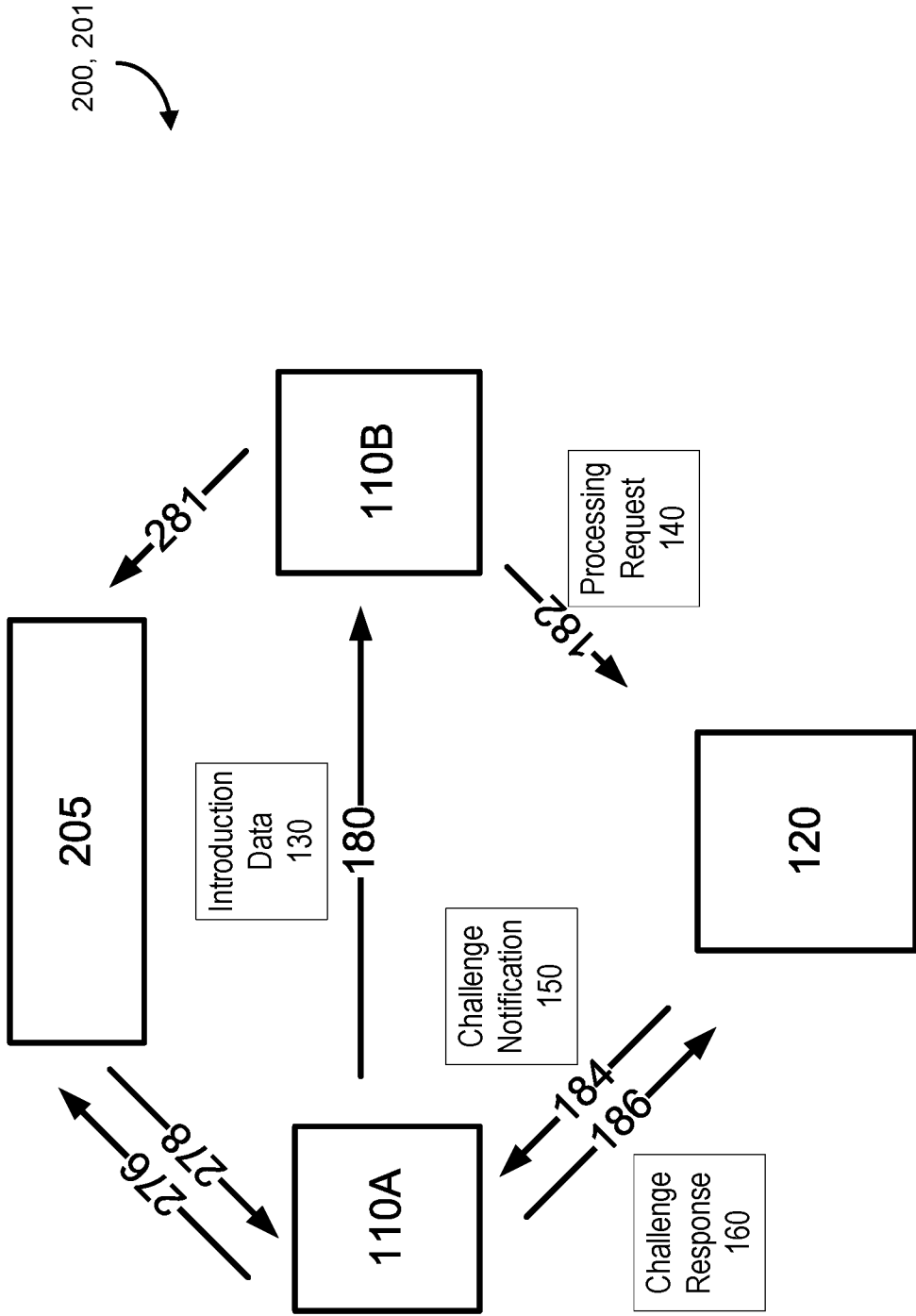


FIG. 2

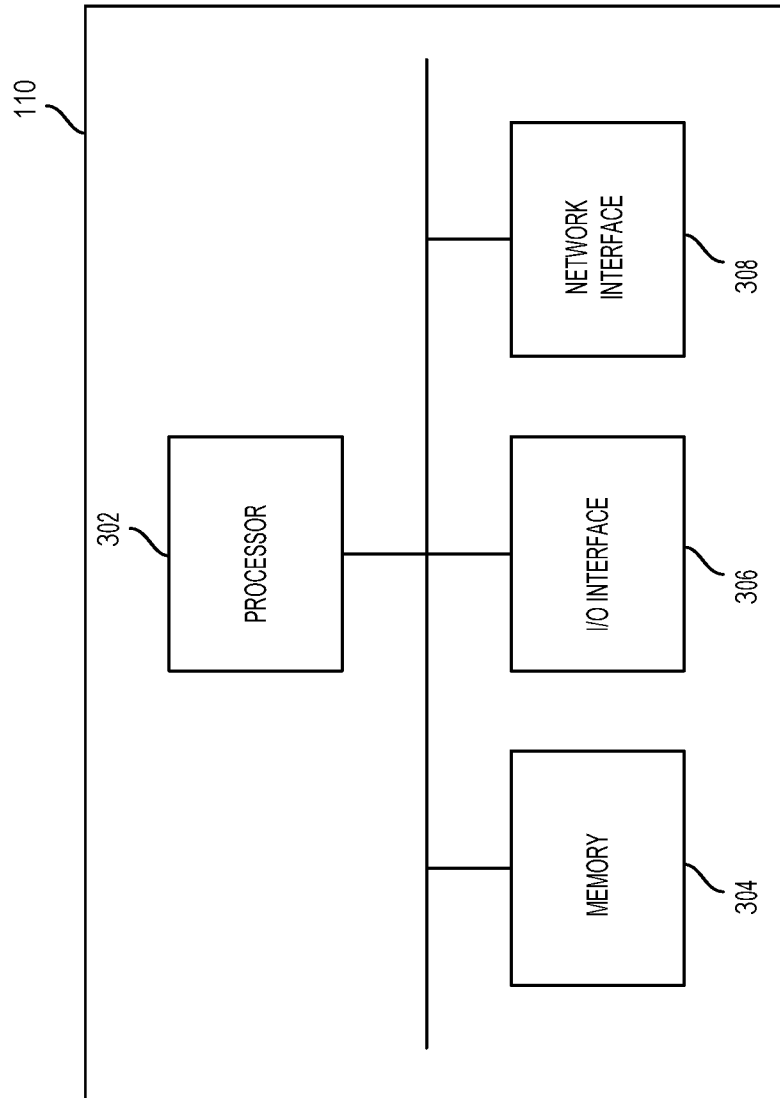


FIG. 3

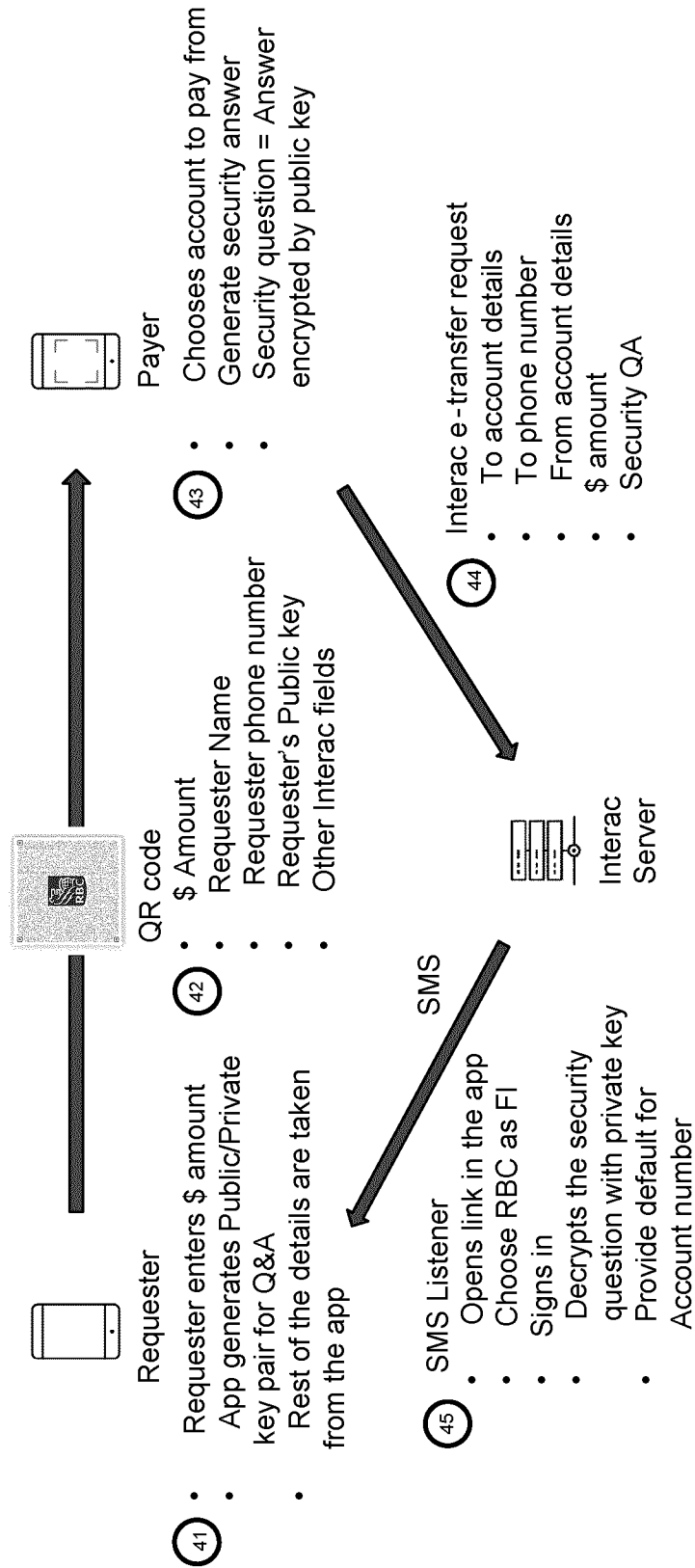


FIG. 4

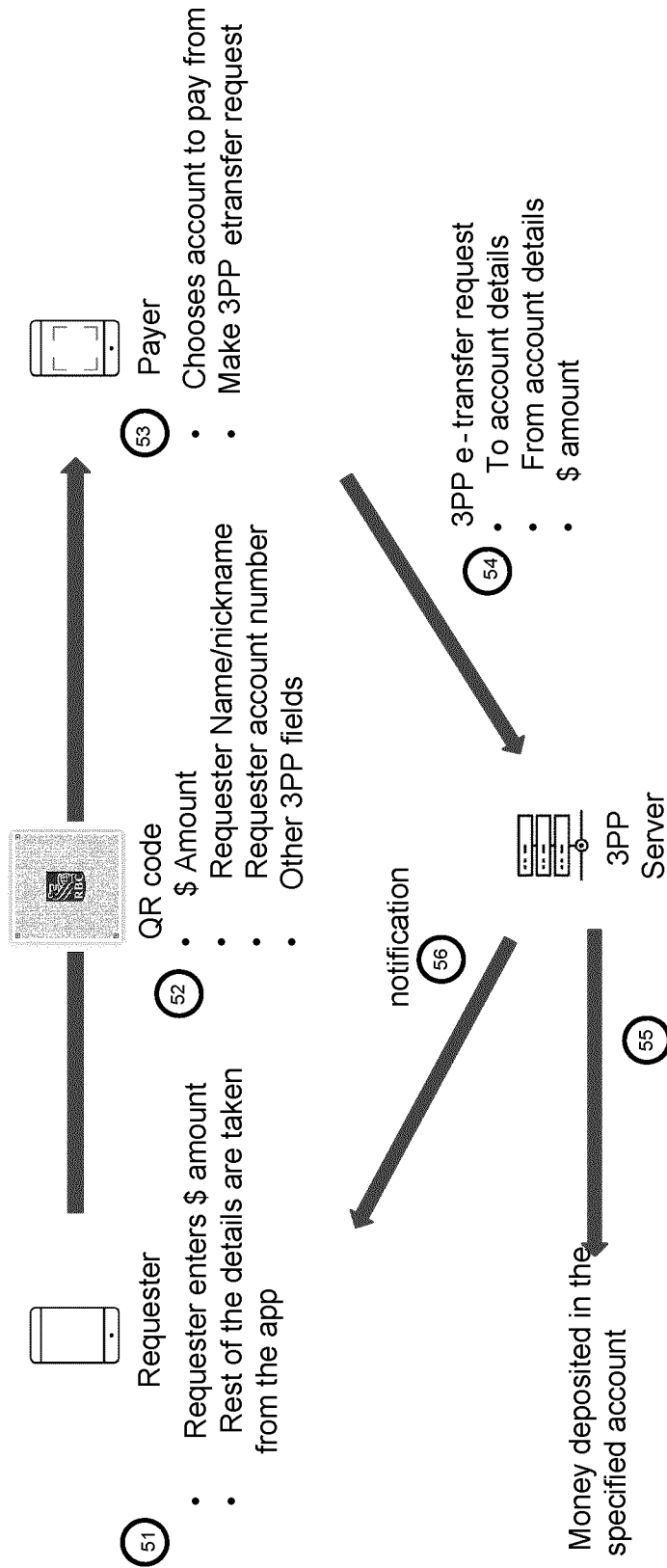


FIG. 5

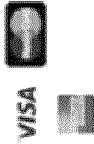
RETAILER123 Clothing

SHIPPING ADDRESS
 DELIVERY OPTIONS
 PAYMENT

3

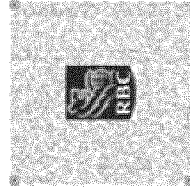
Pay with credit card


RETAILER123 accepts all major credit and debit cards.



Pay with RBC Simba

RETAILER123 now supports payment using RBC Simba!

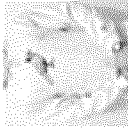




SSL SECURE SHOPPING
YOUR DATA IS SAFE AND SECURE

Edit Cart

SUMMARY (1)



Light Pink Hoodie (Unisex)
Size: S
Quantity: 1
C\$42.50


Subtotal	C\$42.50
Shipping	C\$11.50
Taxes 	C\$0.00
Total	C\$54.00

FIG. 6

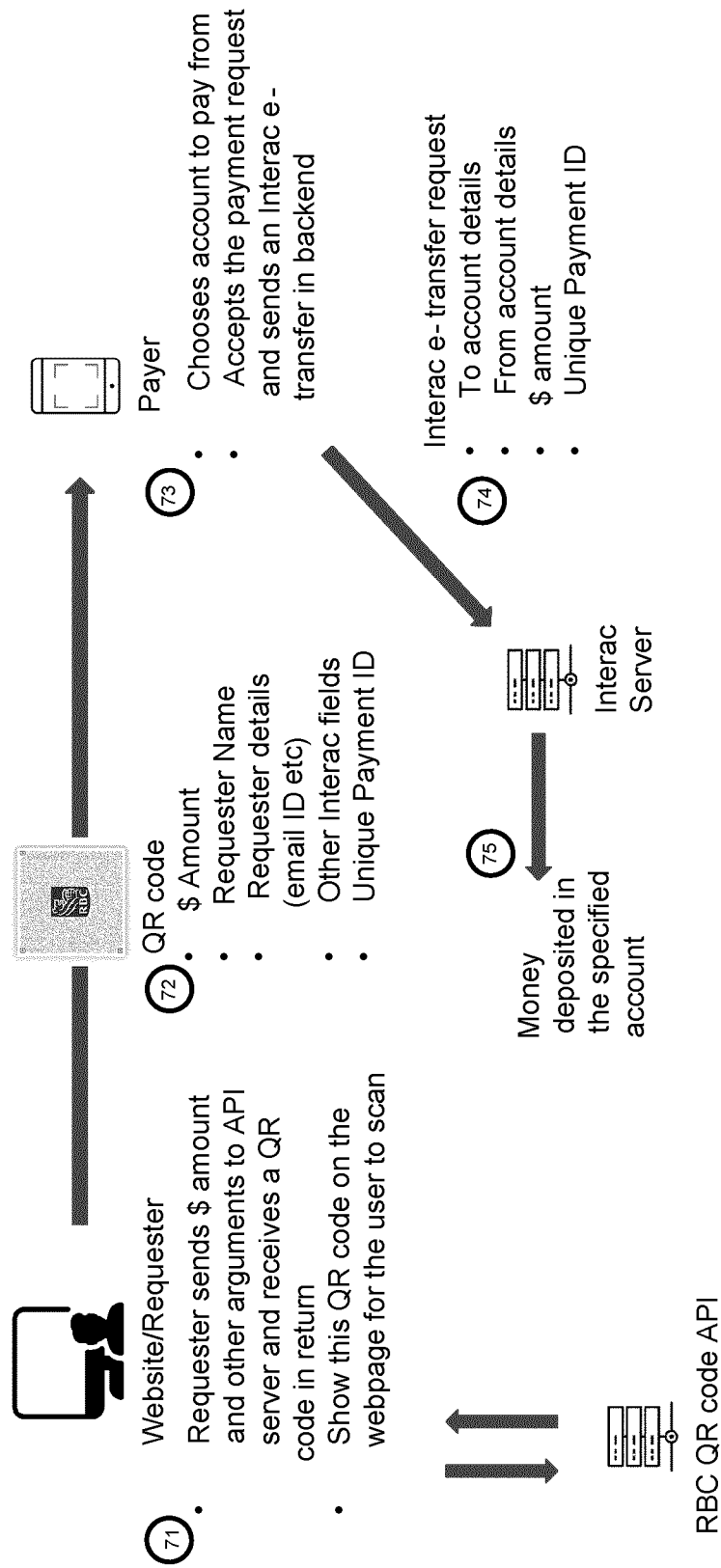


FIG. 7



FIG. 8

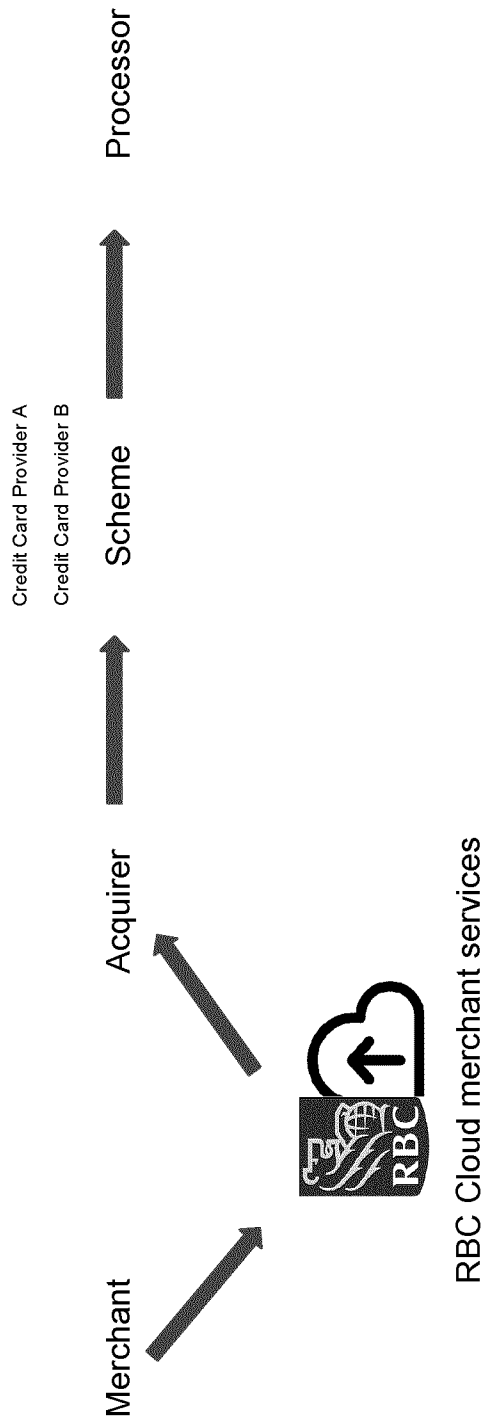


FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2017/051451A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L 9/32** (2006.01), **G06Q 20/10** (2012.01), **H04W 12/06** (2009.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC (2006.01): H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Questel Orbit, Canadian Patent Office Database (Intellect), IEEE Xplore.
Keywords: electr*, interface, proximity, communicat*, channel, encrypt, challenge, decrypt, key, server, initia*.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CA 2 864 030 A1 (Moshir et al.), 29 August 2013 (29-08-2013) *See Abstract, Paragraphs [0009] – [0014], [0064] – [0070], [0091], Figures 1-18	1-38
A	US 7 991 694 B2 (Takayama), 02 August 2011 (02-08-2011) *See Abstract, Column 1 line 29 – Column 3 line 58, Claims 1-4	1-38
A	US 2006/0165060 A1 (Dua), 27 July 2006 (27-07-2006) *See whole document	1-38

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
31 January 2018 (31-01-2018)Date of mailing of the international search report
13 March 2018 (13-03-2018)Name and mailing address of the ISA/CA
Canadian Intellectual Property Office
Place du Portage I, C114 - 1st Floor, Box PCT
50 Victoria Street
Gatineau, Quebec K1A 0C9
Facsimile No.: 819-953-2476Authorized officer

Sajith Bandaranayake (819) 639-5760

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2017/051451

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
CA2864030A1	29 August 2013 (29-08-2013)	CA2864030A1 CA2864030C AU2007267898A1 AU2007267898B2 AU2009228017A1 AU2013222127A1 AU2013222127B2 CA2650852A1 CA2650852C CA2719794A1 CN102037708A EP2021960A2 EP2021960A4 EP2021960B1 EP2286566A1 EP2817984A1 EP2817984A4 EP3023894A1 EP3023894B1 IL208375D0 IL208375A KR20140135997A KR101690850B1 KR20100126850A MX2014010093A MX348109B MX2010010620A MY163154A PH12014501888A1 PH12014501888B1 SG189710A1 SG11201404627VA UA103021C2 US2007293202A1 US7920851B2 US2008133930A1 US8225380B2 US2008109370A1 US8260274B2 US2008108324A1 US8280359B2 US2013252585A1 US8862129B2 US2008167060A1 US8965416B2 US2011151903A1 US9154612B2 US2015072654A1 US9572033B2 US2011145564A1 US9680803B2 US2016044473A1 US9686660B2 US2008081601A1 US9848081B2 US2008214111A1 US2009265552A1 US2012270560A1 WO2007139909A2 WO2007139909A3 WO2008109436A1 WO2009121046A1 WO2013126832A1 ZA201007633B ZA201405967B	29 August 2013 (29-08-2013) 02 May 2017 (02-05-2017) 06 December 2007 (06-12-2007) 14 June 2012 (14-06-2012) 01 October 2009 (01-10-2009) 04 September 2014 (04-09-2014) 07 July 2016 (07-07-2016) 06 December 2007 (06-12-2007) 08 October 2013 (08-10-2013) 01 October 2009 (01-10-2009) 27 April 2011 (27-04-2011) 11 February 2009 (11-02-2009) 28 December 2011 (28-12-2011) 23 December 2015 (23-12-2015) 23 February 2011 (23-02-2011) 31 December 2014 (31-12-2014) 06 January 2016 (06-01-2016) 25 May 2016 (25-05-2016) 22 November 2017 (22-11-2017) 30 December 2010 (30-12-2010) 31 July 2016 (31-07-2016) 27 November 2014 (27-11-2014) 28 December 2016 (28-12-2016) 02 December 2010 (02-12-2010) 18 April 2016 (18-04-2016) 26 May 2017 (26-05-2017) 14 December 2010 (14-12-2010) 15 August 2017 (15-08-2017) 17 November 2014 (17-11-2014) 17 November 2014 (17-11-2014) 31 May 2013 (31-05-2013) 30 October 2014 (30-10-2014) 10 September 2013 (10-09-2013) 20 December 2007 (20-12-2007) 05 April 2011 (05-04-2011) 05 June 2008 (05-06-2008) 17 July 2012 (17-07-2012) 08 May 2008 (08-05-2008) 04 September 2012 (04-09-2012) 08 May 2008 (08-05-2008) 02 October 2012 (02-10-2012) 26 September 2013 (26-09-2013) 14 October 2014 (14-10-2014) 10 July 2008 (10-07-2008) 24 February 2015 (24-02-2015) 23 June 2011 (23-06-2011) 06 October 2015 (06-10-2015) 12 March 2015 (12-03-2015) 14 February 2017 (14-02-2017) 16 June 2011 (16-06-2011) 13 June 2017 (13-06-2017) 11 February 2016 (11-02-2016) 20 June 2017 (20-06-2017) 03 April 2008 (03-04-2008) 19 December 2017 (19-12-2017) 04 September 2008 (04-09-2008) 22 October 2009 (22-10-2009) 25 October 2012 (25-10-2012) 06 December 2007 (06-12-2007) 08 May 2008 (08-05-2008) 12 September 2008 (12-09-2008) 01 October 2009 (01-10-2009) 29 August 2013 (29-08-2013) 27 July 2011 (27-07-2011) 31 August 2016 (31-08-2016)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CA2017/051451

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US7991694B2	02 August 2011 (02-08-2011)	US2009125429A1 US7991694B2 AU8648498A AU761284B2 CN1246941A CN1664828A EP0950968A1 EP0950968A4 EP1467300A1 JP2006040298A JP4181568B2 JP2006031726A JP4181569B2 JP2006053925A JP4264077B2 JP2006040299A JP4264078B2 JP4270475B2 KR20000068758A KR100846553B1 KR20060022734A WO9909502A1	14 May 2009 (14-05-2009) 02 August 2011 (02-08-2011) 08 March 1999 (08-03-1999) 29 May 2003 (29-05-2003) 08 March 2000 (08-03-2000) 07 September 2005 (07-09-2005) 20 October 1999 (20-10-1999) 19 May 2004 (19-05-2004) 13 October 2004 (13-10-2004) 09 February 2006 (09-02-2006) 19 November 2008 (19-11-2008) 02 February 2006 (02-02-2006) 19 November 2008 (19-11-2008) 23 February 2006 (23-02-2006) 13 May 2009 (13-05-2009) 09 February 2006 (09-02-2006) 13 May 2009 (13-05-2009) 03 June 2009 (03-06-2009) 25 November 2000 (25-11-2000) 15 July 2008 (15-07-2008) 10 March 2006 (10-03-2006) 25 February 1999 (25-02-1999)
US2006165060A1	27 July 2006 (27-07-2006)	US2006165060A1 US8700729B2 US2014297438A1 US9235839B2 US2014172724A1 US2014222682A1 US2014337227A1 US2015058227A1 US2015077228A1 US2015081559A1 US2015088750A1 US2015095174A1 US2015095175A1 US2015095235A1 US2015100488A1 US2015100499A1 US2015302413A1 US2015339667A1	27 July 2006 (27-07-2006) 15 April 2014 (15-04-2014) 02 October 2014 (02-10-2014) 12 January 2016 (12-01-2016) 19 June 2014 (19-06-2014) 07 August 2014 (07-08-2014) 13 November 2014 (13-11-2014) 26 February 2015 (26-02-2015) 19 March 2015 (19-03-2015) 19 March 2015 (19-03-2015) 26 March 2015 (26-03-2015) 02 April 2015 (02-04-2015) 02 April 2015 (02-04-2015) 02 April 2015 (02-04-2015) 09 April 2015 (09-04-2015) 09 April 2015 (09-04-2015) 22 October 2015 (22-10-2015) 26 November 2015 (26-11-2015)