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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 September 2014 (18.09.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/141263 A1

(51) International Patent Classification:
G06F 21/31 (2013.01) *G06F 7/04* (2006.01)
G06F 21/00 (2013.01) *H04L 9/32* (2006.01)
G06F 21/30 (2013.01)

(21) International Application Number:
PCT/IL2014/050263

(22) International Filing Date:
13 March 2014 (13.03.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/779,707	13 March 2013 (13.03.2013)	US
61/779,580	13 March 2013 (13.03.2013)	US
61/846,172	15 July 2013 (15.07.2013)	US

(71) Applicant: **BIOTHENT SECURITY LTD.** [IL/IL]; 4 Toscanini Street, 3499304 Haifa (IL).

(72) Inventors: **GREKOV, Evgeny**; 18/8 Kikar Amos a Navi, 7179201 Modiin (IL). **VOLDMAN, Leonid**; 4 Toscanini St., 3499304 Haifa (IL).

(74) Agents: **WEBB & CO.** et al.; P.O. Box 2189, 76121 Rehovot (IL).

(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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: ASYMMETRIC OTP AUTHENTICATION SYSTEM

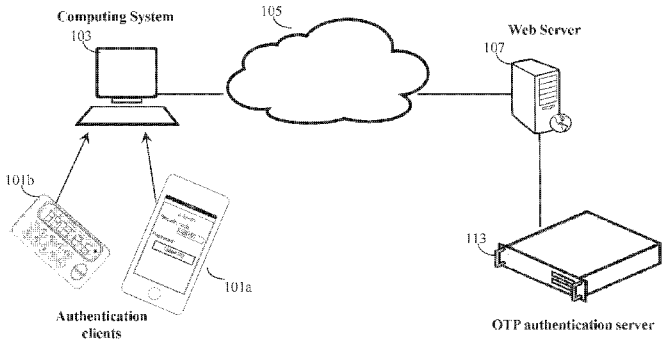

FIG. 1

(57) Abstract: An asymmetric one-time-password (OTP) authentication, biometric authentication and remote directive strong authorization systems are disclosed. The asymmetric OTP authentication system includes a plurality of authentication clients and at last one authentication server. The plurality of authentication clients are configured to generate asymmetric encryption and decryption key pairs and OTP keys and register in the at least one authentication server decryption keys and OTP keys. The plurality of authentication clients are configured to generate OTPs using the OTP keys, to encrypt the generated OTPs using the encryption keys and to generate authentication credentials using encrypted OTPs. The authentication server is configured to decrypt the clients' OTPs using the decryption keys, to generate servers' OTPs using the OTP keys and to authenticate requests by matching decrypted clients' OTPs with server's generated OTPs.

WO 2014/141263 A1

ASYMMETRIC OTP AUTHENTICATION SYSTEM

FIELD OF THE INVENTION

[0001] The invention relates generally to authentication systems and more particularly the invention relates to access authentication, biometric authentication and remote directive strong authorization systems.

BACKGROUND

[0002] Authentication is a foundation service designed to provide information security. It is crucial to authorization and auditing services.

[0003] One time passwords (OTPs) are passwords that are valid for a single authentication session or transaction in contrast to static passwords. OTPs avoid a number of shortcomings that are associated with static passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. A potential intruder, who manages to record an OTP that was already used to log into a service or to conduct a transaction, will not be able to abuse it, since it will be no longer valid.

[0004] Several OTP system implementations are known: Time-based and keyed-hash message authentication code (HMAC/Time)-based OTP (TOPT/HOTP), two-step authentication (2STEP-OTP), Public-key cryptography (PKI)-based two-step authentication (PKI-OTP), Out-of-band authentication - OOB (using alternative channels for OTP delivery, e.g. SMS, e-mail, mobile push, etc.). OOB method depends on permanent availability of secured delivery channels. TOPT/HOTP, 2STEP-OTP and PKI-OTP are communication independent and therefore are more universal methods.

[0005] PKI, refers to a cryptographic algorithm which requires generation of two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaindata and the private key is used to decrypt the cipherdata. The

term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other.

[0006] TOPT/HOTP, 2STEP-OTP and PKI-OTP systems use share secret keys and other synchronized data (e.g. synchronized time, PIN, serial numbers, etc.) as seed input for an OTP algorithm that allows servers to authenticate passwords generated by clients. Thus, TOPT/HOTP, 2STEP-OTP and PKI-OTP systems are vulnerable to shared secrets discovery due to keys thefts, keys leaks, unsecure keys exchange and the like.

[0007] Biometric authentication systems match captured biometric identifiers with specific templates stored in a biometric database repository in order to verify that an individual is the person he or she claims to be. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Examples include, but are not limited to fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, retina odor/scent.

[0008] However, the collection of biometric identifiers stored in a biometric database repository raises privacy concerns about the safety and authorized use of biometric information, concerns that limit a wider use of biometric authentication systems in financial and commercial systems, such as web based businesses and e-commerce.

[0009] Phishing is the act of attempting to acquire information such as usernames, passwords, credit card details and the like by masquerading as a trustworthy entity in an electronic communication. Phishing emails may contain links to websites that are infected with malware. Phishing may be carried out by email spoofing or instant messaging, and it may direct users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

[0010] In view of the above, there is a need for a highly secure OTP authentication and biometric authentication systems. There is further a need for remote directive strong authentication systems designed to prevent phishing attacks.

SUMMARY

[0011] This summary is provided to introduce a selection of concepts in a simplified form that are further described in the detailed description of the invention. According to an aspect of some embodiments of the present invention there is provided an asymmetric OTP authentication system. The asymmetric OTP authentication system may include a plurality of authentication clients and at least one authentication server. The plurality of authentication clients may be configured to generate asymmetric encryption and decryption key pairs and OTP keys, may register in the at least one authentication server the decryption keys and OTP keys. The plurality of authentication clients may be configured to generate OTPs using the OTP keys, to encrypt the generated OTPs using the encryption keys and to provide to the authentication server the encrypted OTPs. The at least one authentication server may be configured to decrypt the clients' OTPs using the decryption keys, to generate servers' OTPs using the OTP keys and to authenticate requests by matching the decrypted authentication clients' OTPs with the server's generated OTPs.

[0012] According to a further feature of an embodiment of the present invention, authentication requests, by the authentication clients, may be single step processes.

[0013] According to a further feature of an embodiment of the present invention, the authentication clients may be configured to initiate registration processes on a plurality of authentication servers.

[0014] According to a further feature of an embodiment of the present invention, the authentication clients may be configured to store in the authentication clients the generated encryption keys.

[0015] According to a further feature of an embodiment of the present invention, the OTPs may be generated using an algorithm such as: RFC 1760 (S/KEY), RFC 2289 (OTP), RFC 4226 (HOTP), RFC 6238 (TOTP) and the like.

[0016] According to a further feature of an embodiment of the present invention, the authentication clients may be: tokens, mobile devices, computing systems and the like.

[0017] According to a further feature of an embodiment of the present invention, the plurality of authentication clients may be further configured to receive biometric inputs, by biometric capable input devices, to generate and store biometric templates in the authentication clients.

[0018] According to a further feature of an embodiment of the present invention, the OTP keys and/or the asymmetric encryption and decryption key pairs may be built upon the stored biometric templates.

[0019] According to a further feature of an embodiment of the present invention, the plurality of authentication clients configured to receive biometric inputs may be further configured to match the biometric inputs with the stored biometric templates and to generate the OTPs if the biometric inputs and the biometric templates match.

[0020] According to a further feature of an embodiment of the present invention, the biometric inputs may be: fingerprints, face images, voice recordings, DNA sequences, palm prints, hand geometries, iris images, retina images and odor, scent recordings and the like.

[0021] According to a further feature of an embodiment of the present invention, the OTP authentication system may be configured to authorize remote directives, wherein approval passwords may be the encrypted OTPs, wherein prior to generating the approval passwords, the plurality of authentication clients may be configured to receive encoded data blocks that may include the remote directives' content, and wherein the generated approval passwords may be generated using the OTP keys, the encryption and decryption keys and the remote directives' content.

[0022] According to a further feature of an embodiment of the present invention, the plurality of authentication clients may include means for receiving the data blocks from terminals and extracting the remote directives' content from the data blocks.

[0023] According to a further feature of an embodiment of the present invention, the plurality of authentication clients may include means for displaying the extracted remote directives' content accompanied with the clients' generated approval passwords.

[0024] According to a further feature of an embodiment of the present invention, the encoded data blocks may be: QR codes, blue tooth, NFC, Wi-Fi transmission, and combination thereof.

[0025] According to a further feature of an embodiment of the present invention, an OTP authentication method is disclosed. The OTP authentication method includes generating, by a plurality of authentication clients, asymmetric encryption and decryption key pairs and OTP keys and registering on at least one authentication server the decryption keys and OTP keys. The methods includes generating authentication credentials, by the plurality of authentication clients, using encrypted OTPs wherein the OTPs may be generated using the OTP keys and encrypted using the encryption keys and authenticating the authentication requests, by the authentication servers, by decrypting the authentication clients' OTPs using the decryption keys, generating servers' OTPs using the OTP keys, and matching the decrypted authentication clients' OTPs with the servers' generated OTPs.

[0026] According to a further feature of an embodiment of the present invention, requesting authentication permits may include transmitting the encrypted OTPs in a single step.

[0027] According to a further feature of an embodiment of the present invention, a biometric asymmetric encrypting OTP authentication method is disclosed. The biometric asymmetric encrypting OTP authentication method may include receiving biometric inputs, by a plurality of authentication clients, by biometric capable input devices, generating and storing biometric templates in the client's devices, generating using the biometric templates, biometric asymmetric encryption and decryption key pairs and OTP keys and registering in at least one authentication server the decryption keys and OTP keys. The method may include matching, by the plurality of authentication clients, biometric inputs with biometric templates. The method may include generating authentication credentials, by plurality of authentication clients, using the encrypted OTPs wherein the OTPs may be generated using the OTP keys and encrypted using the encryption keys. The method may include authenticating the authentication requests, by the authentication servers, by decrypting the clients' OTPs using the decryption keys, generating servers' OTPs

using OTP keys, and by matching the decrypted authentication clients' OTPs with the servers' generated OTPs.

[0028] According to a further feature of an embodiment of the present invention, requesting biometric authentication may include transmitting the encrypted OTPs in a single step.

[0029] According to a further feature of an embodiment of the present invention, a remote-directive strong authorization method is disclosed. The remote-directive strong authorization method may include generating, by a plurality of authentication clients, asymmetric encryption and decryption key pairs and OTP keys and registering on authorization servers, the decryption keys and OTP keys. The method may include transmitting, by the authorization servers, encoded data blocks that include the encoded content of remote directives to the authentication clients. The method may include communicating, by the plurality of authentication clients, encrypted approval passwords generated using the remote directives' content and OTP keys and encrypted by the encryption key. The method may include authorizing the remote directives, by the authorization servers, by decrypting the clients' approval password using the decryption keys, generating servers' approval passwords using the remote directives' content and OTP keys, and by matching the decrypted authentication clients' approval passwords with servers' generated approval passwords.

[0030] According to a further feature of an embodiment of the present invention, the method may include a plurality of terminals used for communicating messages to the authorization servers and for presenting data blocks received from the authorization servers to users.

[0031] According to a further feature of an embodiment of the present invention, the encoded data blocks may be QR codes, blue tooth, NFC, Wi-Fi transmission, and the like.

[0032] Additional features and advantages of the invention will become apparent from the following drawings and description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033] For a better understanding of the invention and to show how the same may be carried into effect, reference will now be made, purely by way of example, to the accompanying drawings in which like numerals designate corresponding elements or sections throughout.

[0034] With specific reference now to the drawings in detail, it is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of the preferred embodiments of the present invention only, and are presented in the cause of providing what is believed to be the most useful and readily understood description of the principles and conceptual aspects of the invention. In this regard, no attempt is made to show structural details of the invention in more detail than is necessary for a fundamental understanding of the invention, the description taken with the drawings making apparent to those skilled in the art how the several forms of the invention may be embodied in practice. In the accompanying drawings:

[0035] FIG. 1 illustrates an asymmetric OTP authentication system architecture, according to certain embodiments;

[0036] FIG. 2 illustrates OTP authentication system asymmetric key pairs' generation and registration, according to certain embodiments;

[0037] FIG. 3 illustrates an overview of an OTP authentication process, according to certain embodiments;

[0038] FIG. 4 illustrates authentication clients' registration on an OTP server, according to certain embodiments;

[0039] FIG. 5 illustrates a single step OTP authentication process, according to certain embodiments;

[0040] FIG. 6 illustrates a flow chart of the OTP authentication process, according to certain embodiments;

[0041] FIG. 7 illustrates authentication client's registration on a plurality of OTP servers, according to certain embodiments;

[0042] FIG. 8 illustrates authentication clients' biometric registration on an OTP server, according to certain embodiments;

[0043] FIG 9 illustrates a biometric OTP authentication process, according to certain embodiments;

[0044] FIG 10 illustrates a flow chart of the biometric OTP authentication process, according to certain embodiments;

[0045] FIG. 11 illustrates a remote directive authorization system's submission form, according to certain embodiments;

[0046] FIG. 12 illustrates a remote directive authorization system's confirmation request, according to certain embodiments;

[0047] FIG. 13 illustrates presenting remote directive's content and the generated approval password on client's display, according to certain embodiments;

[0048] FIG. 14 illustrates submission of the approval password to the application server, according to certain embodiments;

[0049] FIG. 15 illustrates a remote directive strong authorization process, according to certain embodiments;

[0050] FIG. 16 illustrates a flow chart of the remote directive strong authorization process, according to certain embodiments;

[0051] FIG. 17 illustrates a flowchart of an OTP authentication method, according to certain embodiments;

[0052] FIG. 18 illustrates a flowchart of a biometric OTP authentication method, according to certain embodiments; and

[0053] FIG. 19 illustrates a flowchart of a remote directive strong authorization method, according to certain embodiments.

DETAILED DESCRIPTION

[0054] While a number of exemplary aspects and embodiments have been discussed above, those of skill in the art will recognize certain modifications, permutations, additions and subcombinations thereof. It is therefore intended that the following appended claims and claims hereafter introduced be interpreted to include all such modifications, permutations, additions and sub-combinations as are within their true spirit and scope.

[0055] In the description and claims of the application, each of the words "comprise" "include" and "have", and forms thereof, are not necessarily limited to members in a list with which the words may be associated.

[0056] According to certain embodiments of the present invention, an asymmetric OTP authentication system is disclosed. The asymmetric OTP authentication system uses different keys for OTP generation and authentication. Together with shared OTP key, the asymmetric OTP authentication system utilizes asymmetric keys pair, also known as encrypting/decrypting or public/private keys pair, where encrypting key is used for encrypted OTP generation (i.e. authentication credentials) and decrypting key is used for OTP authentication. The asymmetric OTP authentication system includes at least one authentication client and at least one authentication server. The one or more authentication clients are configured to generate asymmetric encryption and decryption key pairs and OTP keys and register on the at least one authentication server the decryption and OTP keys. The one or more authentication clients are configured to generate OTPs using the OTP keys, to encrypt the generated OTPs using the encryption keys and allow authentication using encrypted OTPs in a single authentication step. The authentication servers are configured to decrypt the clients' OTPs using the registered decryption keys, to generate servers' OTPs using the registered OTP keys and to authenticate requests by matching authentication clients' OTPs with server's generated OTPs.

[0057] According to certain embodiments of the present invention, on registration, authentication clients are configured to provide the decryption keys, and not the encryption keys, to the contra-party authentication server. Since encryption keys are generated and stored at the authentication clients, only authentication clients are able to issue authentication credentials (e.g. encrypted OTPs) and hence encryption keys thefts, encryption keys leaks, unsecure encryption keys exchange and the like from authentication servers are impossible.

[0058] According to certain embodiments of the present invention, authentication clients are configured to generate OTPs and encrypt the generated OTPs using encryption keys generated and stored at the authentication clients only.

[0059] As used herein, the terms issued authentication credentials and/or secure codes mean encrypted OTPs that are provided by authentication clients and the terms encrypted OTPs, secure codes and issued credentials are used interchangeably.

As used herein, the terms user name and user ID mean a unique sequence of characters used to identify a user and allow access to a computing system. The terms user name and user ID are used interchangeably herein.

As used herein, the term secure keys means authentication keys, OTP keys, encryption/decryption keys needed to generate and/or validate authentication credentials.

[0060] According to certain embodiments of the present invention, the use of asymmetric encrypted OTPs allows authentication servers to validate that the authentication client that provided credentials for authentication requests is the same authentication client that provided the decryption key on registration since only the encrypting authentication client preserves the encryption key. The encryption keys are created by the authentication clients and are not disclosed at any time to external computing environments.

[0061] Advantageously, embodiments of the present invention facilitate a single step authentication process similar to static password authentication process.

[0062] Another advantage of the asymmetric OTP authentication system is that the use of OTPs prevents man-in-the-middle attacks since OTPs change in each authentication request. Since OTPs are encrypted by the authentication clients and only the authentication client that provided the decryption key on registration preserves the paired encryption key and can generate a valid encrypted OTP, mathematical means cannot be used to crack the authentication keys used to generate the authentication credentials.

[0063] Another advantage of the asymmetric OTP authentication system is that a user name is not required to be stored with the security keys at the authentication client. Hence, even if security keys are stolen they will not be accompanied by the user names in contrast to authentication servers where user names must be linked to security keys and may be both stolen by hackers.

[0064] Optionally, authentication clients' registration processes may be initiated by authentication clients on a plurality of authentication servers and may be re-initiated by the authentication clients.

[0065] According to certain embodiments of the present invention, a biometric asymmetric OTP authentication system is disclosed. A plurality of authentication

clients are configured to receive biometric inputs using biometric capable input devices, to convert biometric inputs into biometric templates and store the biometric templates in the authentication clients' repository, to match biometric inputs with stored biometric templates, to generate encryption and decryption key pairs and OTP keys build upon biometric templates derivatives (e.g. biometric template's digital representation or biometric template's digital signature), to generate OTPs using the generated OTP keys and encrypt OTPs using encryption key. The plurality of authentication clients are configured to issue authentication credentials allowing a single step authentication process. Authentication servers are configured to decrypt authentication credentials using the decryption keys and to generate OTPs using OTP keys. Authentication servers are configured to authenticate received requests by validating the decrypted clients' OTPs with the server's generated OTPs.

[0066] Optionally, the plurality of biometric authentication clients may be configured to generate asymmetric encryption and decryption key pairs and/or OTP keys using biometric inputs and/or biometric templates derivatives.

[0067] Biometric inputs may be fingerprints, face images, voice recordings, DNA sequences, palm prints, hand geometries, iris images, retina images, odor and scent recordings, veins topography and the like.

[0068] According to certain embodiments of the present invention, a remote directives strong authorization system is disclosed. A plurality of authentication clients are configured to generate asymmetric encryption and decryption key pairs and OTP keys and to provide the decryption keys and OTP keys to authorization servers. The plurality of authentication clients are configured to receive encoded data blocks that include the content of remote directives from the authorization servers, to issue encrypted approval passwords based on the remote directives' content and the OTP keys. The authorization servers are configured to decrypt the authentication clients' approval passwords using the decryption keys, to generate servers' approval passwords using the remote directives' content and the OTP keys and to authenticate the remote directives by matching decrypted clients' approval passwords with server's generated approval passwords.

[0069] According to certain embodiments of the present invention, a plurality of terminals are configured to provide data blocks received from authorization servers (by displaying Quick Response (QR) codes for example). QR codes are given as an

example only and Blue Tooth and/or NFC and/or WiFi communication and the like may be used by terminals to provide the data blocks to the authentication clients.

[0070] According to certain embodiments of the present invention, a plurality of authentication clients may be configured to receive the provided data blocks from authorization servers and to present the data blocks' content (i.e. remote directive) to users.

[0071] Reference is now made to FIG. 1, which illustrates an OTP authentication system, according to certain embodiments. OTP authentication system may include a plurality of authentication clients **101a** and **101b** configured to connect to one or more computing systems **103** using their input means further connected through a network **105** to one or more application servers **107**. Application servers **107** may be connected to OTP server **113**.

[0072] Computing system **103** may be a personal computer (PC), a mobile device, an IPAD and the like.

[0073] Authentication clients **101a** and **101b** are configured to issue credentials for web server **107** to be further authenticated by OTP authentication server **113**.

[0074] Reference is now made to FIG. 2, which illustrates OTP authentication system asymmetric key pairs' generation and registration, according to certain embodiments. Authentication client **101**, which may be mobile device and/or tokens for example, may be configured to generate secure key **201** and complementary key **211**. Secure key **201** may includes OTP key **203** and encryption key **205** that may be stored at client **101**. Complementary key **211** may include OTP key **213**, a copy of OTP key **203**, and decryption key **215** that may be registered on OTP server **113**. Encryption key **205** and decryption key **215** are an asymmetric key pair.

[0075] Reference is now made to FIG. 3, which illustrates an overview of an OTP authentication process, according to certain embodiments. Authentication Client **101** may be configured to generate OTPs **310** using OTP key **203**, to encrypt OTPs using encryption key **205** and provide encrypted OTPs to OTP server **113**. OTP server **113** may be configured to generate OTPs **320** using OTP key **213**, which is identical to OTP key **203**. OTP server **113** may be configured to decrypt OTPs

provided by client **101** using registered decryption key **215** and match **330** decrypted clients' OTPs **310** with servers' OTPs **320**.

[0076] Reference is now made to FIG. 4, which illustrates clients' registration on an authentication server, according to certain embodiments. OTP authentication system may include at least one authentication server **113** and a plurality of authentication clients **101a**, **101b** and **101c**. Plurality of authentication clients **101a**, **101b** and **101c** may be configured to generate **402, 404** and **406** asymmetric encryption and decryption key pairs and OTP keys and to register the keys **401, 403** and **405** on the at least one authentication server **113**. Clients **101a**, **101b** and **101c** may be computers, tokens, mobile devices and the like. According to embodiments of the present invention, clients **101a**, **101b** and **101c** may be configured to register the decryption key **215**, OTP key **203** on authentication server **113** and to store the generated encryption key **205**, OTP key **203** in the clients.

[0077] According to embodiments of the present invention, generating and storing the encrypting key at the clients, facilitates an efficient authentication process having a single authentication step similar to static password systems and furthermore, guarantees that only authentication clients are able to generate valid credentials using their keys.

[0078] Reference is now made to FIG. 5, which illustrates a single step OTP authentication process, according to certain embodiments. Single step OTP authentication system **500** includes at least one authentication server **113** and at least one authentication client **101**. Authentication client **101** may be configured to issue credentials for authentication request **(a)** using an encryption key **205** encrypted OTP **203**. Authentication server **113** may be configured to authenticate request **(b)** by decrypting **215** and matching the decrypted authentication request's OTP with a generated OTP using OTP key **203**. Authentication server **113** may be configured to generate OTPs using OTP key **203** stored in authentication server **113**. According to embodiments of the present invention, the information required for authenticating by server **113**, e.g. encrypted OTP and optionally a user ID, may be provided in a single authentication step **(a)** similar to static password authentication systems.

[0079] Reference is now made to FIG. 6, which illustrates a flow chart of the OTP authentication process **600**, according to certain embodiments. Authentication client **101**, may be configured to generate OTP using OTP key **203** and encrypt the generated OTP using encryption key **205 (FIG. 3)**. OTP server **113** may be configured to draw the user's registered decryption key **215** and OTP key **213** from a repository stored in the OTP server using user name **605**. OTP server **113** may be configured to receive the client's encrypted OTP **603** to decrypt the client's OTP **609** using decryption key **215**. OTP server **113** may be configured to generate OTP **611** using the registered OTP key **213**.

[0080] Optionally, OTP Server **113** and authentication client **101** may be configured to generate OTPs using the synchronized clock and other synchronized data (not shown).

[0081] OTP server **113** may be configured to match **613** the client's decrypted OTP **609** with the authentication server's generated OTP **611**. OTP authentication server **113** may be configured to authenticate the request **615** if the two OTPs match **614.**

[0082] Optionally, OTPs may be generated, by authentication clients and servers, using algorithms such as RFC 1760 (S/KEY), RFC 2289 (OTP), RFC 4226 (HOTP), RFC 6238 (TOTP), combinations of thereof and the like.

[0083] According to embodiments of the present invention, authentication client **101** is configured to generate valid encrypted OTPs using OTP key **203** and encryption key **205**. Since encryption key **205** is generated and stored at, authentication client **101**, encryption key **205** cannot be stolen or leak out from authentication server **113**.

[0084] Reference is now made to FIG. 7, which illustrates client's registration on a plurality of authentication servers **700**, according to certain embodiments. Authentication client **101**, may be configured to register on a plurality of authentication servers **113**, **115** and **117**. Authentication client **101**, may be configured to generate identical or diverse sets of decryption/encryption keys and OTP keys **701** for each one of the OTP authentication servers and register them in each OTP servers **113**, **115** and **117**.

[0085] Authentication client **101**, may be configured to store for each server **113**, **115** and **117** encryption keys (**715**, **725** and **735**) and OTP keys (**713**, **723** and **733**) during the authentication client's registrations **703**, **705** and **707** on OTP servers **113**, **115** and **117**.

[0086] Proposed biometric authentication systems use biometric identifiers repository to store biometric images/templates of users recorded on registration/enrollment procedure. In contrast to traditional biometric database repository systems, according to certain embodiments of the present invention, biometric identifiers are stored in authentication clients and not in centralized database repositories. Authentication clients are configured to store and match biometric inputs and to generate OTPs that may be authenticated by authentication servers that are not required to store any biometric identifiers.

[0087] According to embodiments of the present invention, biometric templates are stored at the authentication clients only. Furthermore, storing the encrypting keys only at the authentication clients prevents stealing the encrypting keys from authentication servers. Finally, storing the encryption keys at the authentication clients allows a single step authentication process similar to static password authentication systems.

[0088] Reference is now made to FIG. 8, which illustrates clients' registration **800** on an OTP server, according to certain embodiments. Plurality of authentication clients **101a**, **101b** and **101c** may be configured to receive biometric inputs **802**, **812** and **822** by biometric capable devices **852**, **862** and **872** that may be included in authentication clients **101a**, **101b** and **101c** or may be external devices. The plurality of clients **101a**, **101b** and **101c** may be configured to generate **803**, **813** and **823** biometric templates from the biometric inputs and to store the generated biometric templates in the clients on enrolment.

[0089] Biometric inputs may be fingerprints, face images, voice recordings, DNA sequences, palm prints, hand geometries, iris images, retina images, odor and scent recordings. However, any biometric input known in the art may be used and such biometric inputs are in the scope of the present invention.

[0090] Plurality of authentication clients **101a**, **101b** and **101c** may be configured to generate asymmetric encryption and decryption key pairs (**806** and **808**, **816** and **818**, **826** and **828**) and OTP keys (**804**, **814** and **824**) that may be built upon

the generated biometric templates. Plurality of authentication clients **101a**, **101b** and **101c** may be configured to provide **805**, **815** and **825** decryption keys (**808**, **818** and **828**), OTP keys (**804**, **814** and **824**) to OTP server **113** and to store the generated encryption keys (**806**, **816** and **826**) and OTP keys in the authentication clients.

[0091] Optionally, the plurality of authentication clients may be configured to generate asymmetric encryption and decryption key pairs and/or OTP keys using the biometric inputs and/or the biometric templates.

[0092] Reference is now made to FIG. 9, which illustrates a biometric OTP authentication process, according to certain embodiments. Biometric OTP authentication system **900** may include at least one authentication server **113** and at least one authentication client **101**. Authentication client **101** may be configured to issue credentials for biometric authentication request **(a)** using encrypted OTP **901**. OTP server **113** may be configured to authenticate the biometric authentication request **(b)** by matching the decrypted clients' authentication request's OTP with OTP server's **113** generated OTP. OTP server **113** may be configured to generate OTPs using OTP keys stored in the authentication server on registration. According to embodiments of the present invention, the OTP authentication process may be a single step authentication process where the information required for biometric authentication may be provided in a single step **(a)**.

[0093] Reference is now made to FIG. 10, which illustrates a flow chart of biometric authentication process **1000**, according to certain embodiments. Authentication client **101a**, may be configured to receive biometric input **802** from biometric capable devices **852** and may be configured to match biometric input **802** with a stored biometric template **1001** generated on registration. If matching **1002**, client **101a** may be configured to generate an OTP and to encrypt it **1004** using encryption key **806** generated on registration. OTP **1004** may be generated using OTP key **804**.

[0094] OTP server **113** may be configured to draw user's decryption key **808** and OTP key **804** from the server repository using user ID **1006**. OTP server **113** may be configured to receive the client's encrypted OTP **1005** and to decrypt the client's OTP **1009** using decryption key 808. OTP server **113** may be configured to generate OTP **1011** using OTP key **804**.

[0095] Optionally, OTP server **113** and client **101a** may be configured to generate OTP 1011 and 1004 using in addition to OTP key **804** and also synchronized clock and other synchronized data (not shown).

[0096] OTP server **113** may be configured to match **1013** the client's decrypted OTP **1009** with the server's generated OTP **1011**. OTP server **113** may be configured to authenticate the requested biometric authentication **1014** if the two OTPs match **1013**.

[0097] Phishing techniques attempt to substitute content of users remote directives transmitted over a network by masquerading as a trustworthy entity in the remote directive transmission chain. Phishing techniques may attempt to change remote directives' amounts and receiver's identity in bank transfers or payment orders, change items type and buyer details in purchase orders and the like.

[0098] According to embodiments of the present invention, approval passwords, generated in both authentication clients and authorization servers, among other security keys, are based on the remote directives' content. Phishing attempts may be prevented since the approval passwords that are based on the remote directives' content will not match if the remote directive content is changed by a man-in-the-middle-attack or other means. Furthermore, according to embodiments of the present invention, authentication clients may be configured to receive data blocks by means of QR codes (blue tooth, Wi-Fi communication, NFC and the like) that are generated by authorization servers that include the remote directive contents and to present the contents to users. Thus, users may validate that the content of their remote directives have not been changed using a phishing or other malware techniques, which makes the present invention's authorization system a strong authorization system.

[0099] Reference is now made to FIG. 11, which illustrates a remote directive authorization system's submission form, according to certain embodiments. A remote directive's submission form **1101** may include payment order information, such as Name: Mr. John Smith for example, Account: 123-456789/A and Amount: $15.45 for example.

[00100] Submission form **1101** may appear on terminal's screen where the terminal may be configured to transmit the submission form **(a)** to web server **107**.

Optionally, Submission form **1101** may appear on any kind of computing system's display.

[00101] Reference is now made to FIG. 12, which illustrates a remote directive authorization system's confirmation request, according to certain embodiments. Application server **107** may be configured to transmit a confirmation request with data block in plain form or encrypted **(b)** to client **101a** that contains the remote directives content in a QR code **1201** representation that may be displayed on computing system screen FIG. 1, **103** for example.

[00102] Reference is now made to FIG. 13, which illustrates presenting remote directive's content and the generated approval password on client's display, according to certain embodiments. Authentication client **101a** (shown in FIG. 12) may be configured to scan the QR code **1301**, extract the directive content from the scanned QR code and present **1509** the content on authentication client's **101a** display to a user. The remote directive content that may include for example Name: Mr. John Smith, Account: 123-456789/A, Amount: $15.45 may be presented to the user accompanied by an approval password **1303**.

[00103] The approval password, **753847** for example, is the remote directive's content dependent OTP. According to embodiments of the present invention, the remote directive's content dependent approval password is generated by authentication client **101a** using client's OTP key (FIG. 2, **203**) and is further encrypted by an encryption key (FIG. 3, **205**).

[00104] Reference is now made to FIG. 14, which illustrates submission of an approval password to application server **107**, according to certain embodiments. Authentication client **101a** may be configured to provide the remote directive's content dependent approval password **(c)** to application server **107** through terminal **1203**. To complete the remote directive authorization process, authorization server (not shown) may be configured to decrypt the received remote directive's content dependent OTP **(c)** using decryption key FIG. 3, **215**, to generate a remote directive's content dependent approval password using a registered OTP key (FIG.3, **213**) and to match decrypted client's OTPs and Server's generated OTP as illustrated in FIG. 15 below.

[00105] Reference is now made to FIG. 15, which illustrates a remote directive strong authorization process, according to certain embodiments. Remote directive strong authorization system **1500** may include at least one authorization server **1501** and at least one authentication client **101**. Authentication client **101** may be configured to generate encryption and decryption keys and OTP keys and register the OTP and decryption keys on at least one authorization server **1501**. Authentication client **101** may be configured to store the decryption key and OTP key in authorization server **1501** and to store the generated encryption key and OTP key in authentication client **101**.

[00106] Authorization server **1501** may be configured to provide to authentication client **101** encoded data blocks **1503** that include remote directives' contents **1502.** The provided encoded data blocks **1510** may be for example in form of QR codes **1503** (e.g. 2D barcodes). Authentication client **101** may be configured to decode encoded blocks **1504** and to present the encoded blocks' content **1506** to users accompanied with encrypted OTP **1505**, which is encrypted by encryption key **205** generating approval password **1509**. Authentication client **101** may be configured to provide **1520** the encrypted approval password **1509** to authorization sever **1501**. Authorization server **1501** may be configured to authorize remote directives **1530** by matching **1508** decrypted authentication clients' communicated approval passwords with server's generated approval passwords **1507**.

[00107] Reference is now made to FIG. 16, which illustrates a flow chart of the remote directive authorization process **1600**, according to certain embodiments. Authorization server **1501**, is configured to receive **1603** a remote directive **1601.** Authorization server **1501** may be configured to encode the remote directive's content in data block in form of QR code **1605** and to provide the QR code **1510** to authentication client **101** (e.g. by displaying it on directive terminal's screen).

[00108] Authentication client **101**, may be configured to scan the QR code **1607** and to display the content of the remote directive encoded in the QR code to the user **1609** for validation. Authentication client **101** may be configured to generate approval passwords using OTP key **203** and the remote directives' content **1611**. Authentication client **101** may be configured to encrypt approval passwords using

encryption key FIG. 3, **203** and may be configured to provide **1520** the encrypted approval passwords **1611** for authorization on authorization server **1501**.

[00109] Authorization Server **1501** may be configured to draw the user's decryption key **215** and OTP key **213** from the authorization server **1501** repository using user name **1604**.

[00110] Authorization server **1501** may be configured to decrypt approval passwords **1613** using decryption key **215**. Authorization server **1501** may be configured to generate server's approval passwords **1615** using OTP key **213** and the remote directive content **1606.**

[00111] Optionally, authorization server **1501** and client **101** may be configured to generate the server's and client's approval passwords **1615** and **1611** using the synchronized data e.g. clock and the like (not shown). Authorization server **1501** may be configured to match **1617** the decrypted client's approval passwords **1613** with the server's generated approval passwords **1615**. Authorization server **1501** may be configured to authorize **1530** the client's remote directive **1601** if the two approval passwords match **1617.**

[00112] FIG. 17 illustrates a flowchart of an OTP authentication method, according to certain embodiments. OTP authentication method **1700** includes: in stage **1710,** generating, by a plurality of authentication clients, asymmetric encryption and decryption key pairs and OTP keys and registering on authentication servers the decryption keys and OTP keys; in stage **1720**, requesting authentication permits, by using credentials generated by plurality of authentication clients, using encrypted OTPs wherein the OTPs are generated using the OTP keys and encrypted by the encryption keys; in stage **1730**, approving the authentication requests, by the authentication servers, by matching the decrypted client's OTPs with the server's generated OTPs.

[00113] OTP authentication method **1700** stage **1720** includes a single step authentication that may include further communicating users IDs to the authentication server.

[00114] OTP authentication method **1700** stage **1730** may include decrypting the authentication request credentials using the decryption keys and generating OTPs using the OTP keys.

[00115] FIG. 18 illustrates a flowchart of biometric OTP authentication method, according to certain embodiments. Biometric OTP authentication method **1800** includes: in stage **1810,** receiving biometric inputs, by a plurality of authentication clients, using biometric capable input devices, generating and storing biometric templates in the authentication client's devices, generating asymmetric encryption and decryption key pairs and OTP keys and registering on authentication servers the decryption keys and OTP keys; in stage **1820,** matching, by a plurality of authentication clients, biometric inputs with biometric templates; in stage **1830,** requesting authentication permits using authentication credentials, e.g. encrypted biometric OTPs, wherein the authentication credentials are generated using the OTP keys and encrypted by the encryption keys; in stage **1840,** authenticating the authentication requests by matching the decrypted client's OTPs with the server's generated OTPs.

[00116] Biometric OTP authentication method **1800** stage **1810** generating asymmetric encryption and decryption key pairs and OTP keys may include generating the keys using the biometric templates.

[00117] Biometric OTP authentication method **1800** stage **1830** includes a single step authentication that may include further communicating users IDs to the authentication server.

[00118] Biometric OTP authentication method **1800** stage **1840** may include, by the authentication server, decrypting the authentication credentials using the decryption keys and generating OTPs using the OTP keys.

[00119] FIG. 19 illustrates a flowchart of remote directive strong authorization method, according to certain embodiments. Remote directive OTP strong authorization method **1900** includes: in stage **1910,** generating, by a plurality of clients, asymmetric encryption and decryption key pairs and OTP keys and registering on authorization servers the decryption keys and OTP keys; in stage **1920,** transmitting, by the authorization servers, encoded data blocks that include remote directives' content to authentication clients; in stage **1930,** communicating, by the plurality of authentication clients, encrypted approval password based on the remote directives' content and the OTP keys; in stage **1940,** authorizing the remote directives

by matching decrypted clients' approval passwords with servers' generated approval passwords.

[00120] Remote directive strong authorization method **1900** stage **1940** may include decrypting clients' approval passwords using decryption keys and generating approval passwords using remote directives' content and OTP keys.

[00121] Remote directive strong authorization method **1900** plurality of authentication clients may include a plurality of terminals configured to communicating messages to authorization servers and to presenting data blocks (e.g. QR codes) received from the authorization servers to users.

[00122] Advantageously, the above described OTP authentication system may be used to authenticate in a single step similar to static password authentication systems.

[00123] Another advantage of the above described OTP authentication system is that authentication clients are configured to encrypt credentials using encryption keys, generated and stored only in the authentication clients, and thus the encryption keys are not provided to authentication servers and hence cannot be stolen or leak from authentication servers.

[00124] Advantageously, the above described biometric OTP authentication system may be used for biometric authentication without storing biometric identifiers in biometric database repositories.

[00125] Another advantage of the above described biometric OTP authentication system is that biometric authentication may be a single step authentication similar to static password authentication systems.

[00126] Advantageously, the above described remote directive strong authorization system may be used to authorize remote directives and prevent phishing attacks by the usage of encrypted approval passwords that is based on the remote directive content and OTP keys.

[00127] Another advantage of the above described remote directive authorization system is that it is a strong authentication system that use asymmetric encryption and decryption key pairs to encrypt and decrypt OTPs, e.g. the approval passwords, and furthermore use the content of the remote directives as additional security factor when generating the approval passwords.

[00128] Although the invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, it is intended to embrace all such alternatives, modifications and variations that fall within the spirit and broad scope of the appended claims.

[00129] It is appreciated that certain features of the invention, which are, for clarity, described in the context of separate embodiments, may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable sub-combination.

[00130] Unless otherwise defined, all technical and scientific terms used herein have the same meanings as are commonly understood by one of ordinary skill in the art to which this invention belongs. Although methods similar or equivalent to those described herein can be used in the practice or testing of the present invention, suitable methods are described herein. In addition, the methods and examples are illustrative only and not intended to be limiting.

[00131] It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather the scope of the present invention is defined by the appended claims and includes both combinations and sub-combinations of the various features described hereinabove as well as variations and modifications thereof, which would occur to persons skilled in the art upon reading the foregoing description. While preferred embodiments of the present invention have been shown and described, it should be understood that various alternatives, substitutions, and equivalents can be used, and the present invention should only be limited by the claims and equivalents thereof.

What is claimed is:

1. An asymmetric OTP authentication system, the system comprising:

a plurality of authentication clients and at least one authentication server,

wherein said plurality of authentication clients are configured to generate asymmetric encryption and decryption key pairs and OTP keys, register in said at least one authentication server said decryption keys and OTP keys,

wherein said plurality of authentication clients are configured to generate OTPs using said OTP keys, to encrypt said generated OTPs using said encryption keys and to provide to said authentication server said encrypted OTPs,

wherein said at least one authentication server is configured to decrypt said clients` OTPs using said decryption keys, to generate servers' OTPs using said OTP keys and to authenticate requests by matching said decrypted authentication clients' OTPs with said server's generated OTPs.

2. The system according to claim 1, wherein authentication requests, by said authentication clients, are single step processes.

3. The system according to claim 1, wherein said authentication clients are configured to initiate registration processes on a plurality of authentication servers.

4. The system according to claim 1, wherein said authentication clients are configured to store in said authentication clients said generated encryption keys.

5. The system according to claim 1, wherein said OTPs are generated using an algorithm selected from the group consisting of: RFC 1760 (S/KEY), RFC 2289 (OTP), RFC 4226 (HOTP), RFC 6238 (TOTP), and combinations thereof.

6. The system according to claim 1, wherein said authentication clients are selected from the group consisting of: tokens, mobile devices, computing systems and combinations of thereof.

7. The system according to claim 1, wherein said plurality of authentication clients are further configured to receive biometric inputs, by biometric capable input devices, to generate and store biometric templates in said authentication clients.

8. The system according to claim 7, wherein said OTP keys and/or said asymmetric encryption and decryption key pairs are built upon said stored biometric templates.

9. The system according to claim 8, wherein said plurality of authentication clients configured to receive biometric inputs are further configured to match said biometric inputs with said stored biometric templates and to generate said OTPs if said biometric inputs and said biometric templates match.

10. The system according to claim 9, wherein said biometric inputs are selected from the group consisting of: fingerprints, face images, voice recordings, DNA sequences, palm prints, hand geometries, iris images, retina images and odor and scent recordings.

11. The system according to claim 1, wherein said OTP authentication system is configured to authorize remote directives, wherein approval passwords are said encrypted OTPs, wherein prior to generating said approval passwords, said plurality of authentication clients are configured to receive encoded data blocks that include the remote directives' content, and wherein said generated approval passwords are generated using said OTP keys, said encryption and decryption keys and said remote directives' content.

12. The system according to claim 11, wherein said plurality of authentication clients further comprising means for receiving said data blocks from terminals and extracting said remote directives' content from said data blocks.

13. The system according to claim 12, wherein said plurality of authentication clients further comprising means for displaying said extracted remote directives' content accompanied with said clients' generated approval passwords.

14. The system according to claim 11, wherein said encoded data blocks are selected from the group consisting of: QR codes, blue tooth, NFC, Wi-Fi transmission and combination thereof.

15. An asymmetric one-time-password (OTP) authentication method, the method comprising:

generating, by a plurality of authentication clients, asymmetric encryption and decryption key pairs and OTP keys and registering on at least one authentication server said decryption keys and OTP keys;

generating authentication credentials, by said plurality of authentication clients, using encrypted OTPs wherein said OTPs are generated using said OTP keys and encrypted using said encryption keys; and

authenticating said authentication requests, by said authentication servers, by decrypting said authentication clients' OTPs using said decryption keys, generating servers' OTPs using said OTP keys, and matching said decrypted authentication clients' OTPs with said servers' generated OTPs.

16. The method according to claim 15, wherein said requesting authentication permits comprising transmitting said encrypted OTPs in a single step.

17. A biometric asymmetric encrypting one-time-password (OTP) authentication method, the method comprising:

receiving biometric inputs, by a plurality of authentication clients, by biometric capable input devices, generating and storing biometric templates in said client's devices, generating using said biometric templates, biometric asymmetric encryption and decryption key pairs and OTP keys and registering in at least one authentication server said decryption keys and OTP keys;

matching, by said plurality of authentication clients, biometric inputs with biometric templates

generating authentication credentials, by plurality of authentication clients, using said encrypted OTPs wherein said OTPs are generated using said OTP keys and encrypted using said encryption keys; and

authenticating said authentication requests, by said authentication servers, by decrypting said clients' OTPs using said decryption keys, generating servers' OTPs using OTP keys, and by matching said decrypted authentication clients' OTPs with said servers' generated OTPs.

18. The method according to claim 17, wherein said requesting biometric authentication comprising transmitting said encrypted OTPs in a single step;

19. A remote-directive strong authorization method, the method comprising:

generating, by a plurality of authentication clients, asymmetric encryption and decryption key pairs and OTP keys and registering on authorization servers, said decryption keys and OTP keys;

transmitting, by said authorization servers, encoded data blocks that include the encoded content of remote directives to said authentication clients;

communicating, by said plurality of authentication clients, encrypted approval passwords generated using said remote directives' content and OTP keys and encrypted by said encryption key;

authorizing said remote directives, by said authorization servers, by decrypting said clients' approval password using said decryption keys, generating servers' approval passwords using said remote directives' content and OTP keys, and by matching said decrypted authentication clients' approval passwords with servers' generated approval passwords.

20. The method according to claim 19, further comprising a plurality of terminals used for communicating messages to said authorization servers and for presenting data blocks received from said authorization servers to users.

21. The method according to claim 19, wherein said encoded data blocks are QR codes, blue tooth, NFC, Wi-Fi transmission and combination thereof.

5

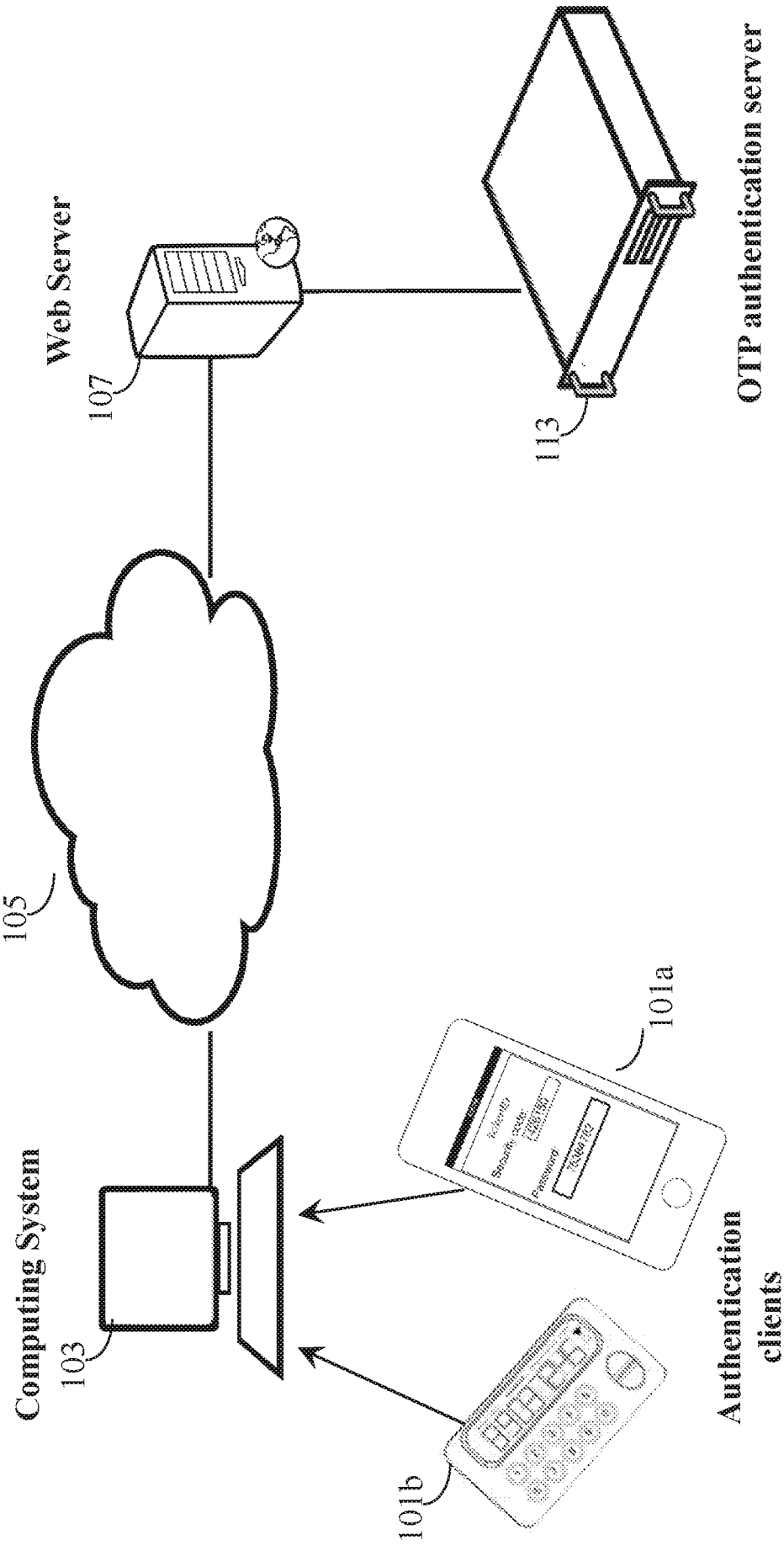
Web Server
107
OTP authentication server
113
105
Computing System
103
101a
Authentication clients
101b

FIG. 1

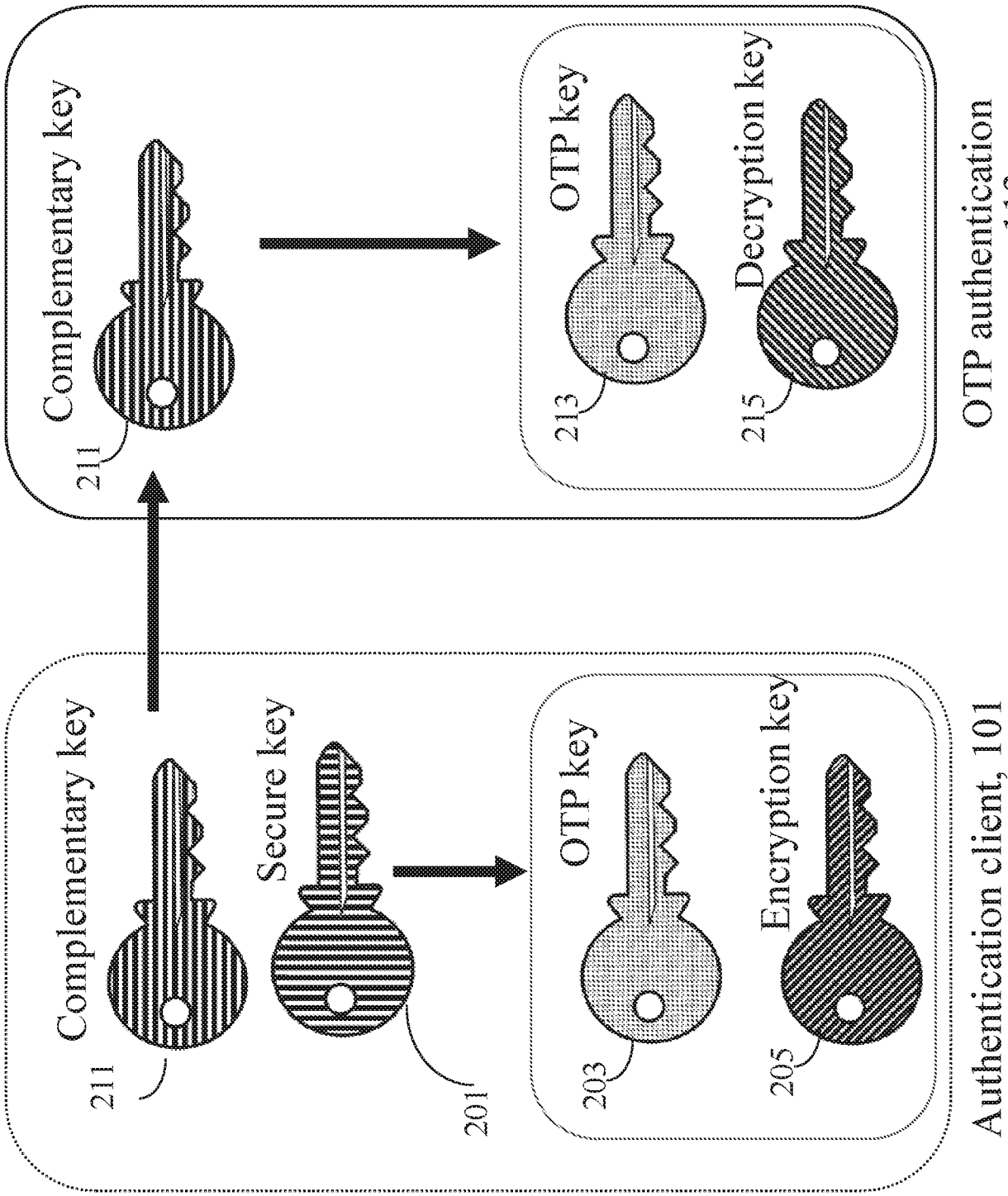
Complementary key
211
Secure key
201
OTP key
203
Encryption key
205
Authentication client, 101
Complementary key
211
OTP key
213
Decryption key
215
OTP authentication server, 113

FIG. 2

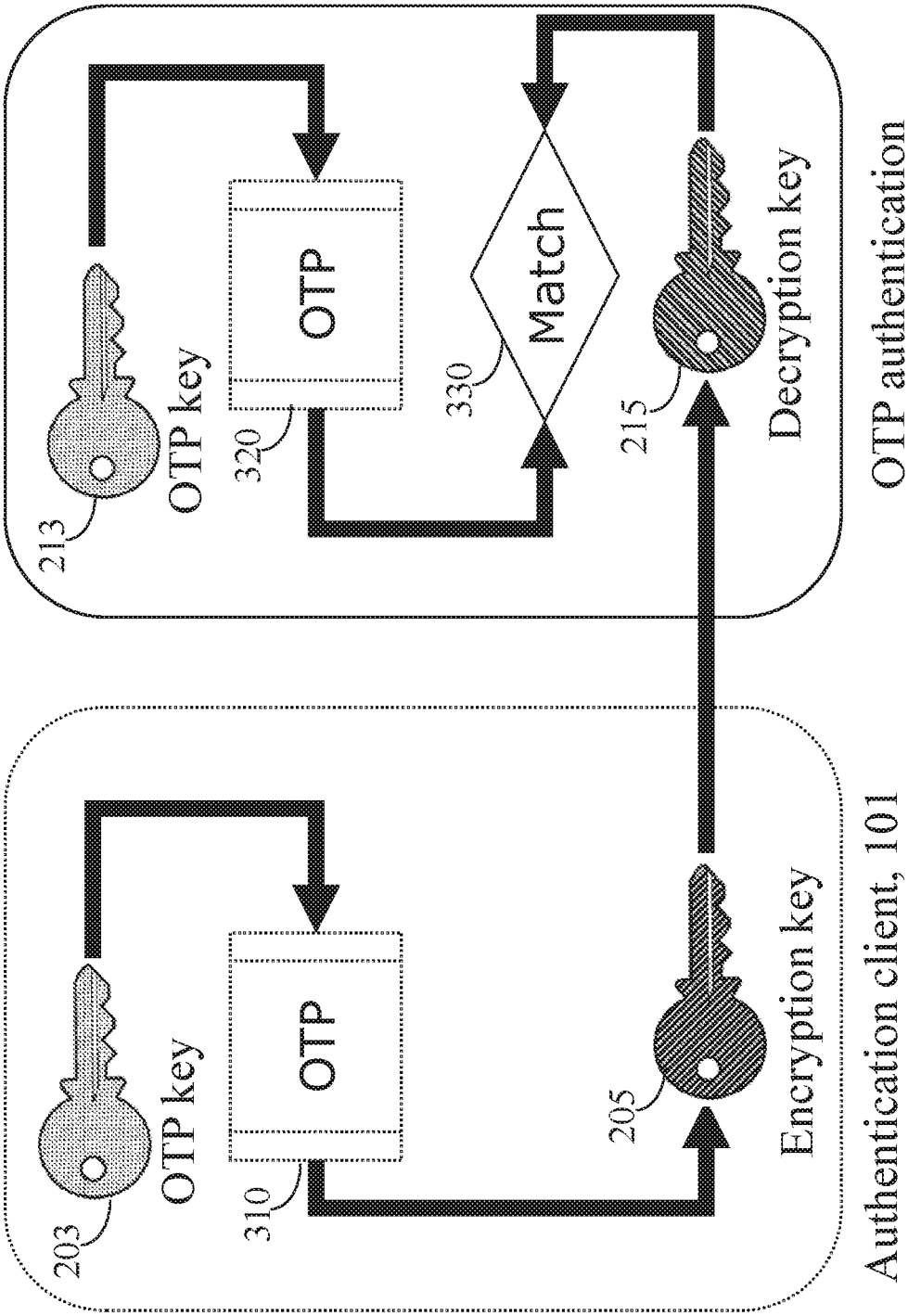
OTP key
213
OTP
320
Match
330
Decryption key
215
OTP authentication server, 113
OTP key
203
OTP
310
Encryption key
205
Authentication client, 101

FIG. 3

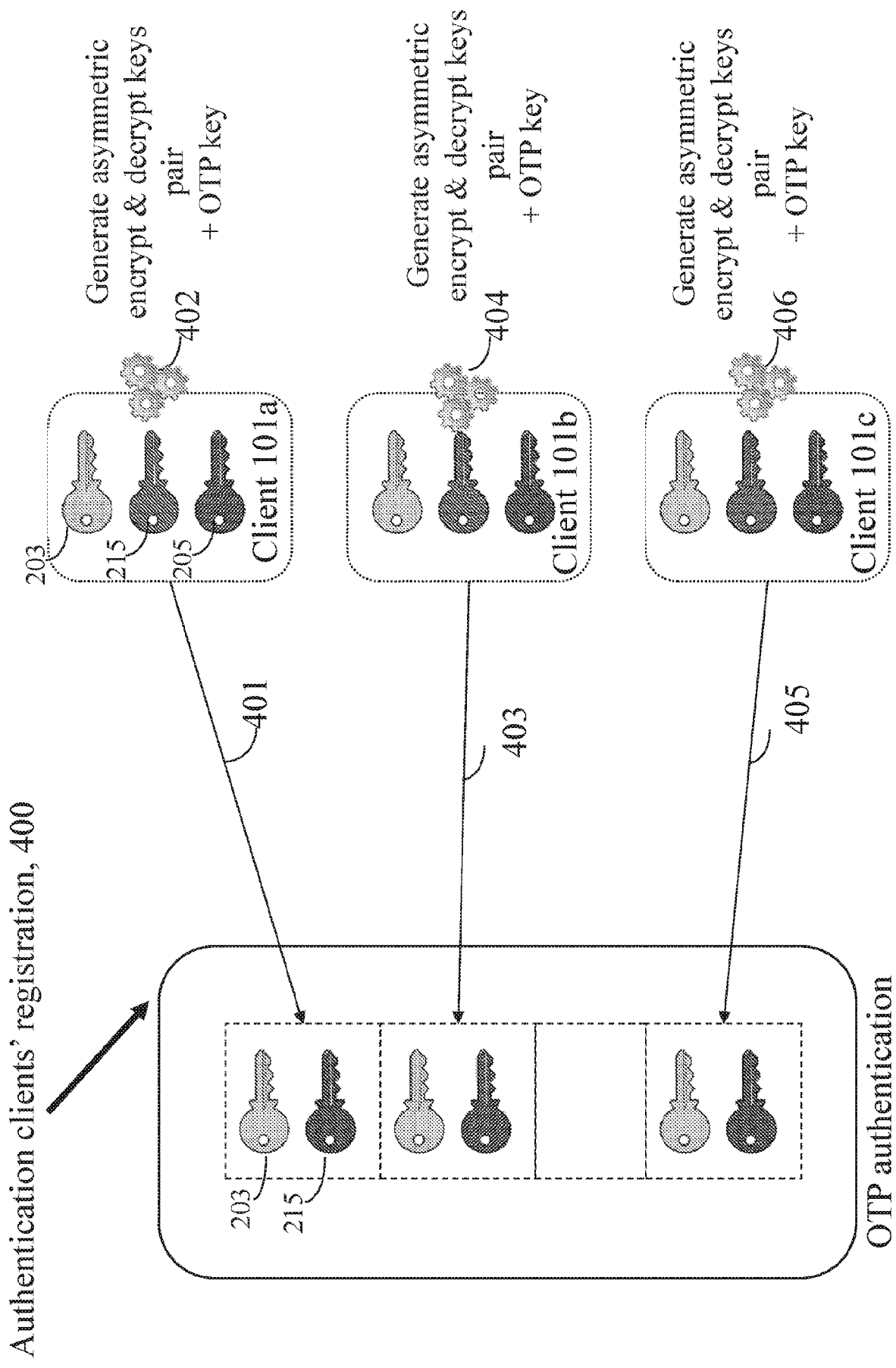
Authentication clients' registration, 400
Generate asymmetric encrypt & decrypt keys pair + OTP key
402
Client 101a
203
215
205
401
Generate asymmetric encrypt & decrypt keys pair + OTP key
404
Client 101b
403
Generate asymmetric encrypt & decrypt keys pair + OTP key
406
Client 101c
405
OTP authentication server, 113
203
215

FIG. 4

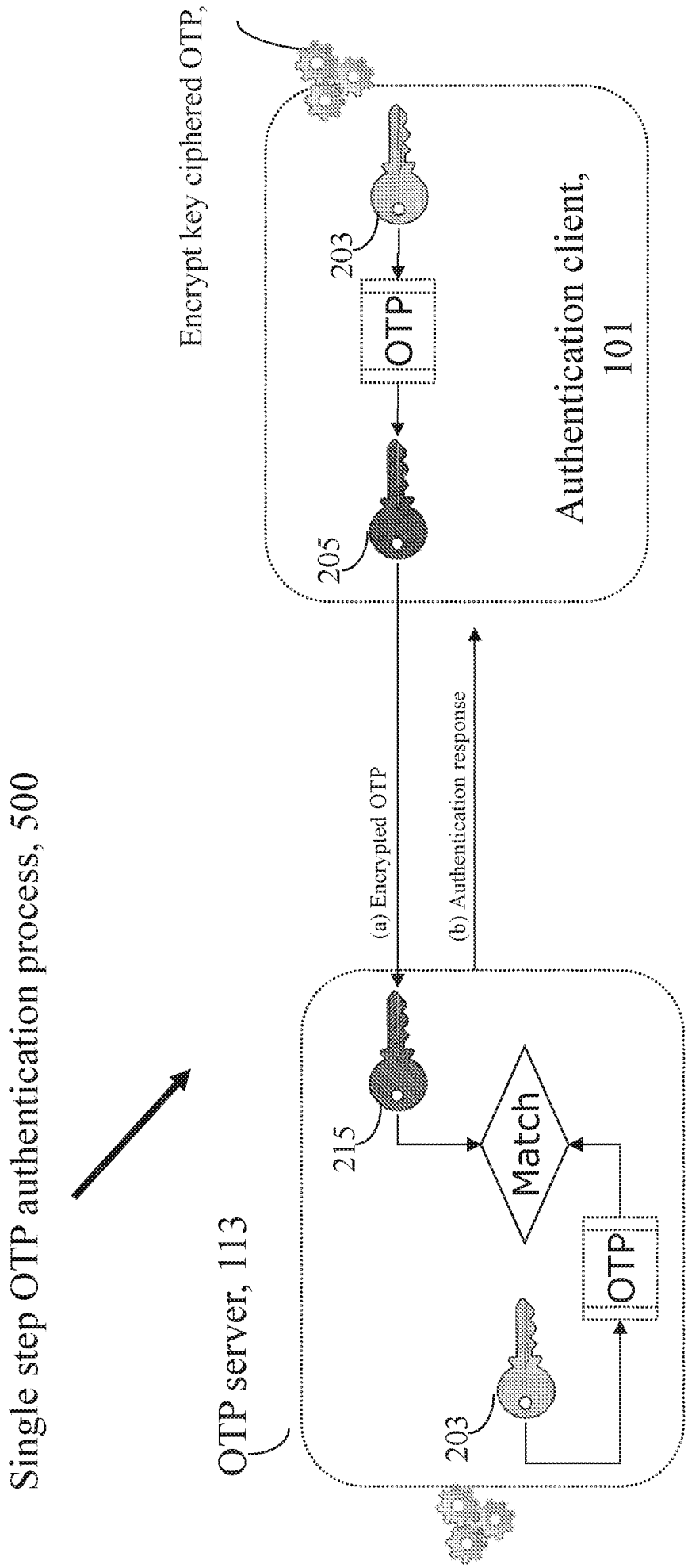
Single step OTP authentication process, 500
OTP server, 113
Encrypt key ciphered OTP,
Authentication client,
101
203
OTP
205
(a) Encrypted OTP
(b) Authentication response
215
Match
OTP
203

FIG. 5

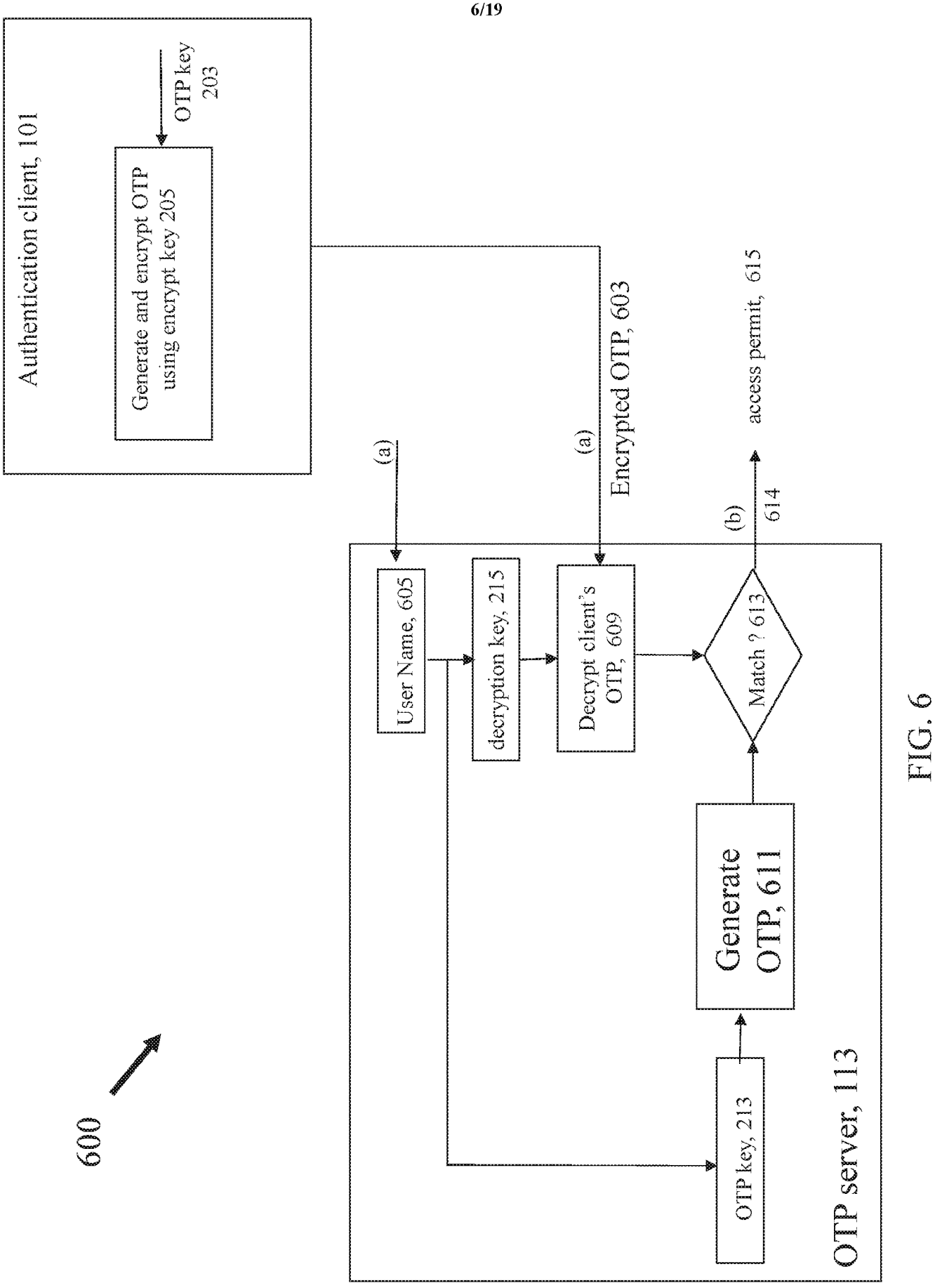
600
Authentication client, 101
Generate and encrypt OTP using encrypt key 205
OTP key 203
(a)
Encrypted OTP, 603
(b)
access permit, 615
614
User Name, 605
decryption key, 215
Decrypt client's OTP, 609
Match ? 613
Generate OTP, 611
OTP key, 213
OTP server, 113

FIG. 6

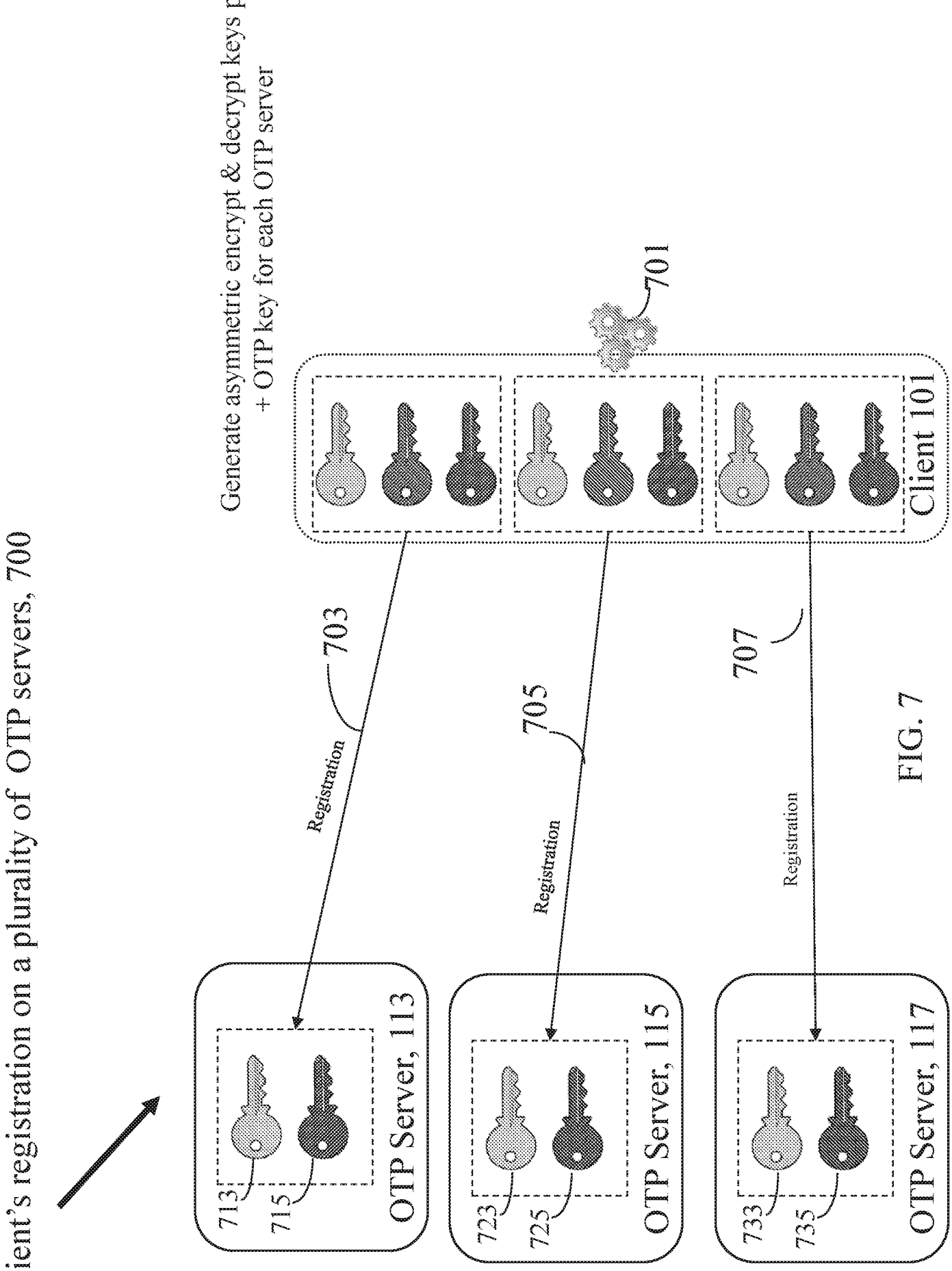
Client's registration on a plurality of OTP servers, 700
Generate asymmetric encrypt & decrypt keys pair
+ OTP key for each OTP server
701
Client 101
703
705
707
Registration
Registration
Registration
713
715
OTP Server, 113
723
725
OTP Server, 115
733
735
OTP Server, 117

FIG. 7

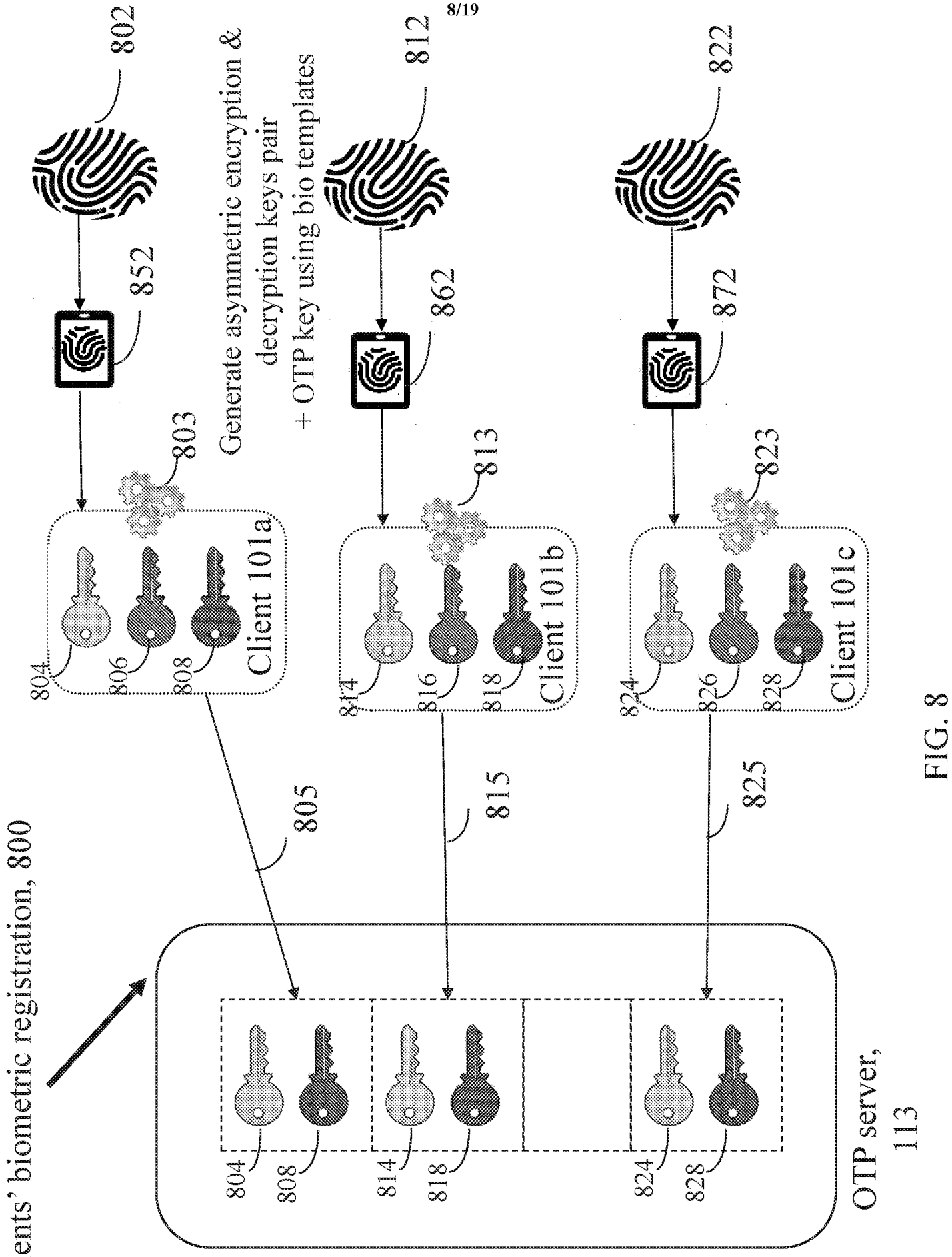
Clients' biometric registration, 800
802
852
803
Generate asymmetric encryption & decryption keys pair + OTP key using bio templates
804
806
808
Client 101a
805
812
862
813
814
816
818
Client 101b
815
822
872
823
824
826
828
Client 101c
825
OTP server, 113

FIG. 8

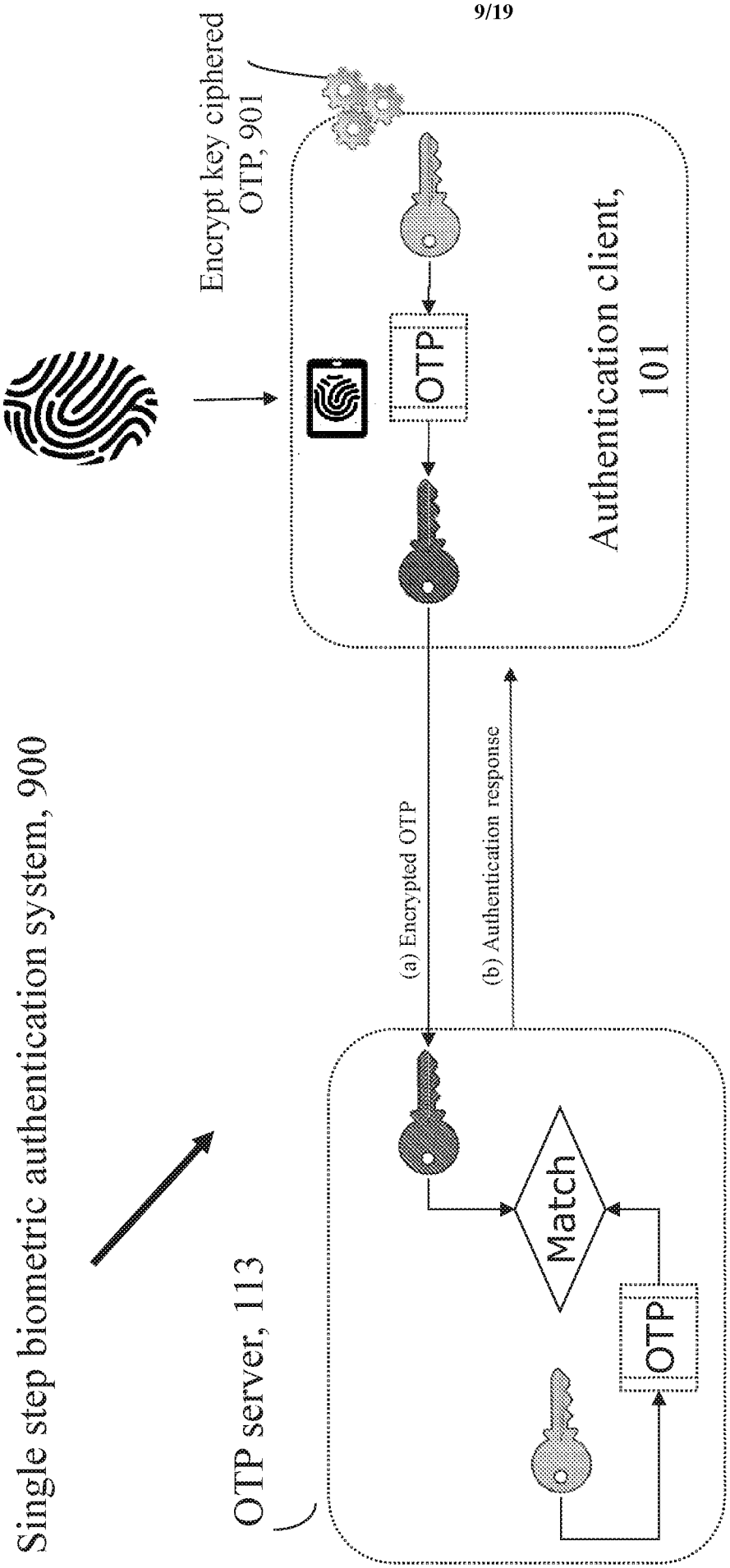
Single step biometric authentication system, 900
OTP server, 113
Match
OTP
(a) Encrypted OTP
(b) Authentication response
Authentication client, 101
OTP
Encrypt key ciphered OTP, 901

FIG. 9

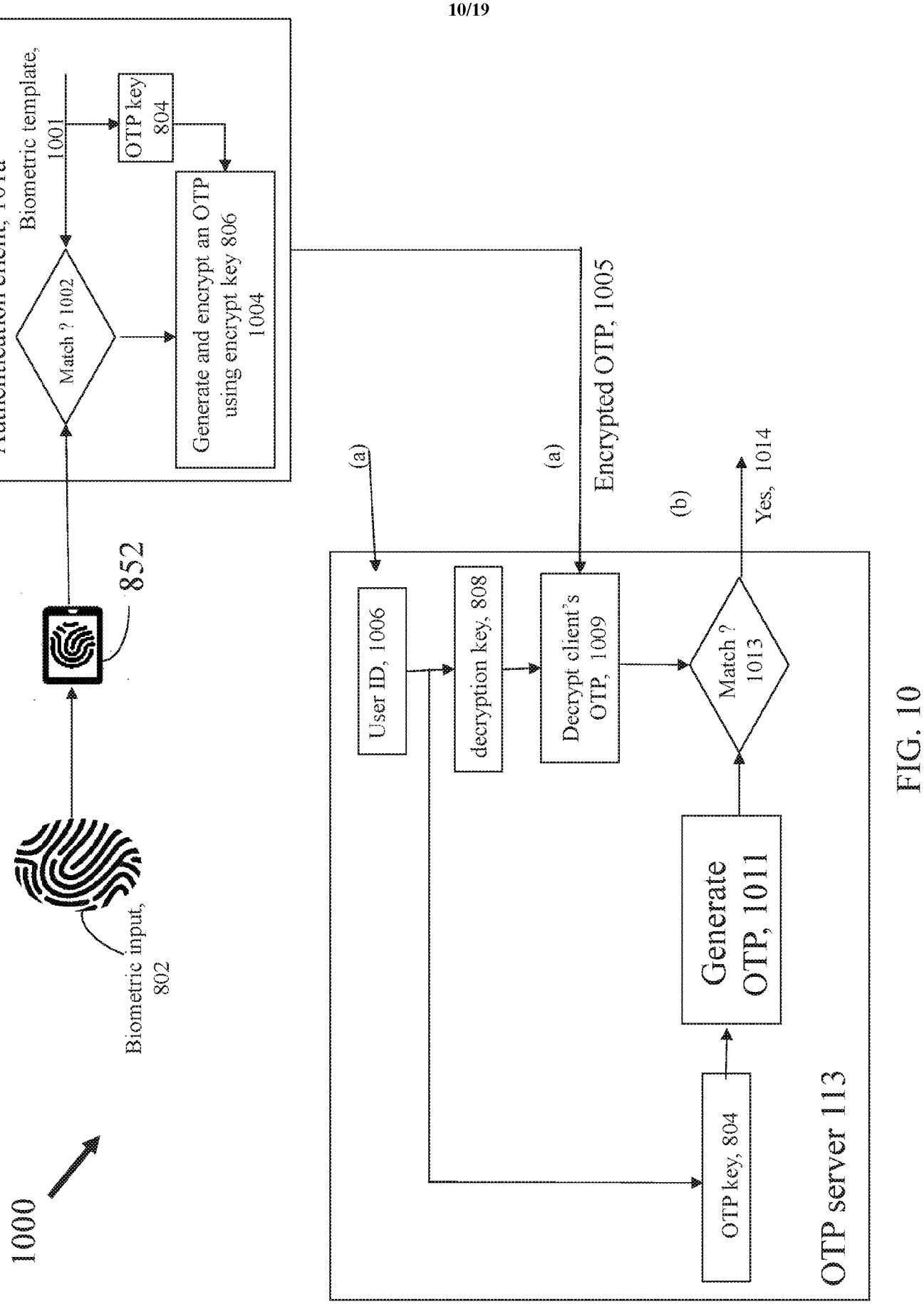
1000
Biometric input, 802
852
Authentication client, 101a
Biometric template, 1001
Match ? 1002
OTP key 804
Generate and encrypt an OTP using encrypt key 806 1004
(a)
Encrypted OTP, 1005
(a)
(b)
Yes, 1014
User ID, 1006
decryption key, 808
Decrypt client's OTP, 1009
Match ? 1013
Generate OTP, 1011
OTP key, 804
OTP server 113

FIG. 10

1101
http://payment order
Payment order
Receiver:
Name:
John Smith
Account:
123-456789/A
Amount:
$15.45
Send
a
Submission form
107
101a

FIG. 11

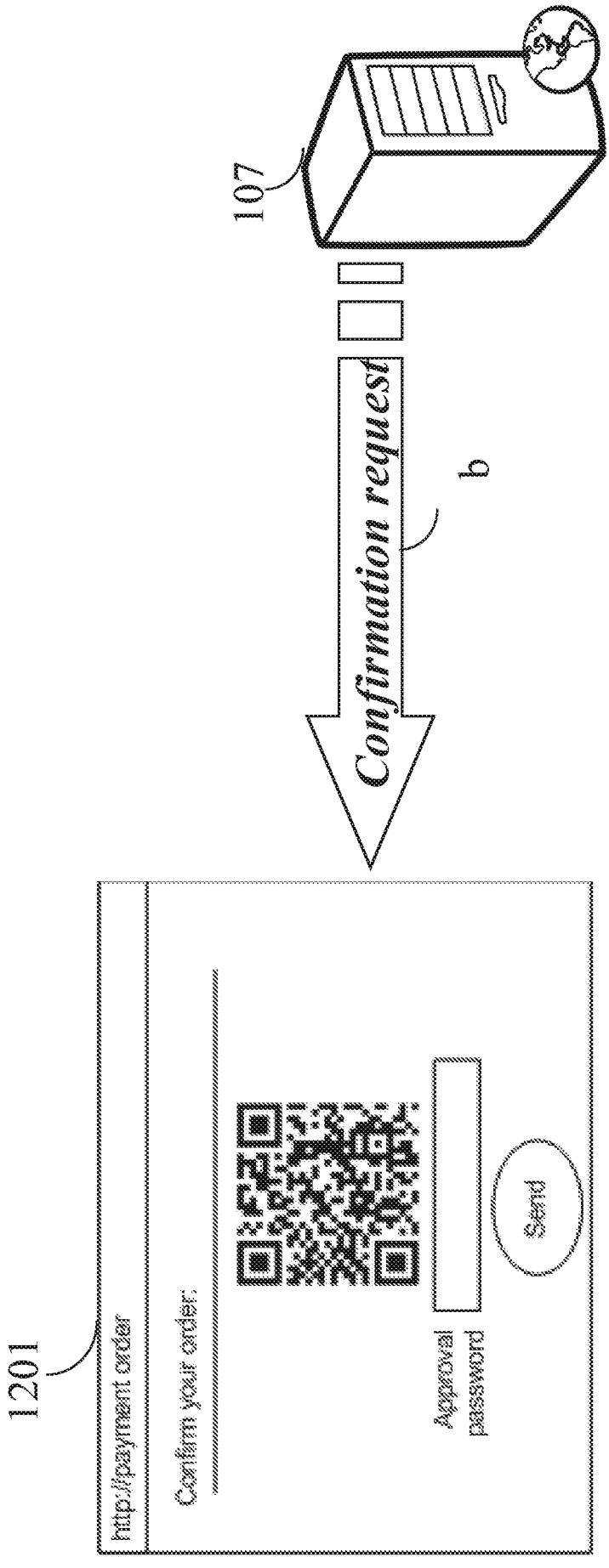
107
Confirmation request
b
1201
http://payment order
Confirm your order:
Approval password
Send
101a

FIG. 12

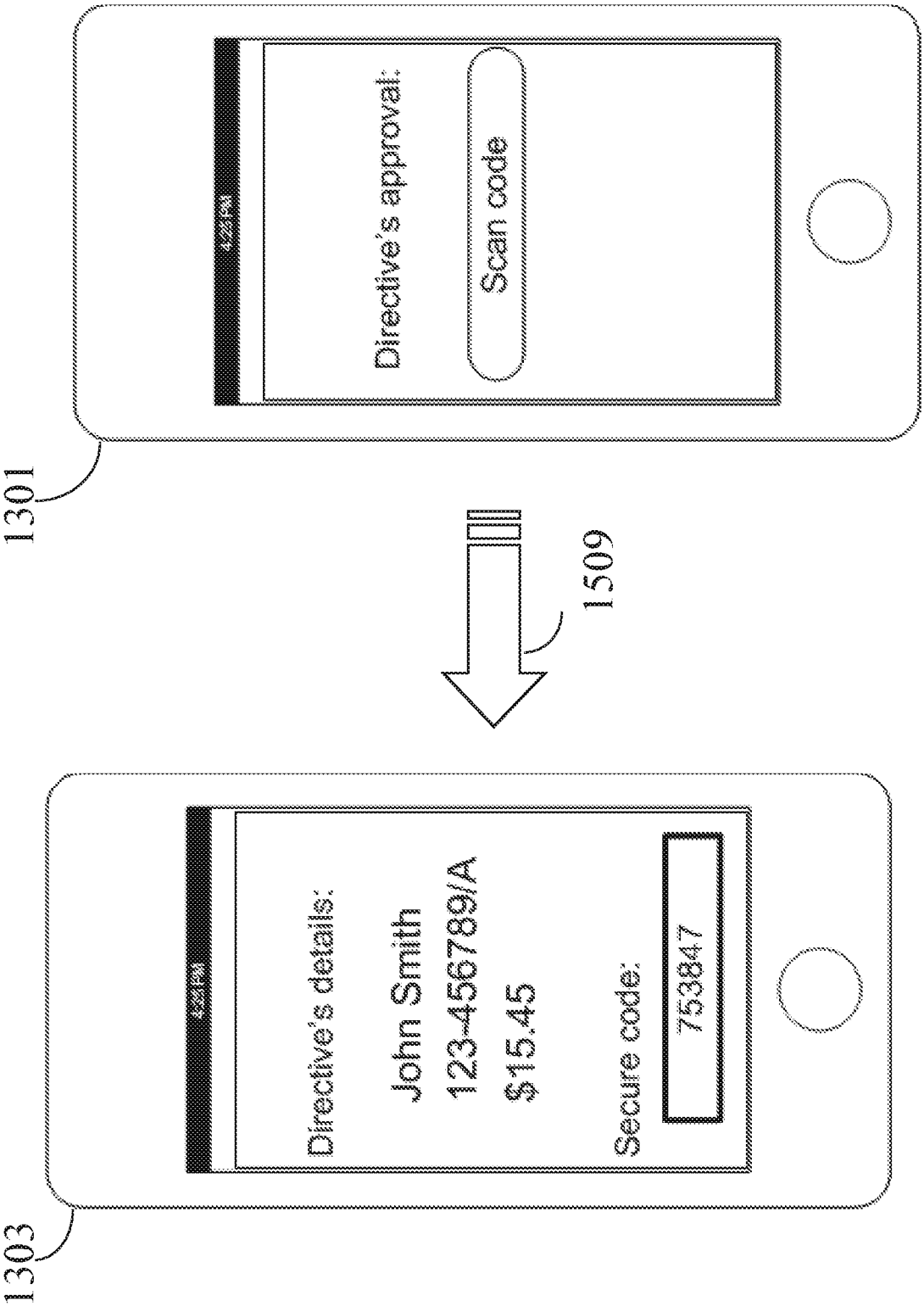
1301
Directive's approval:
Scan code
1509
1303
Directive's details:
John Smith
123-456789/A
$15.45
Secure code:
753847

FIG. 13

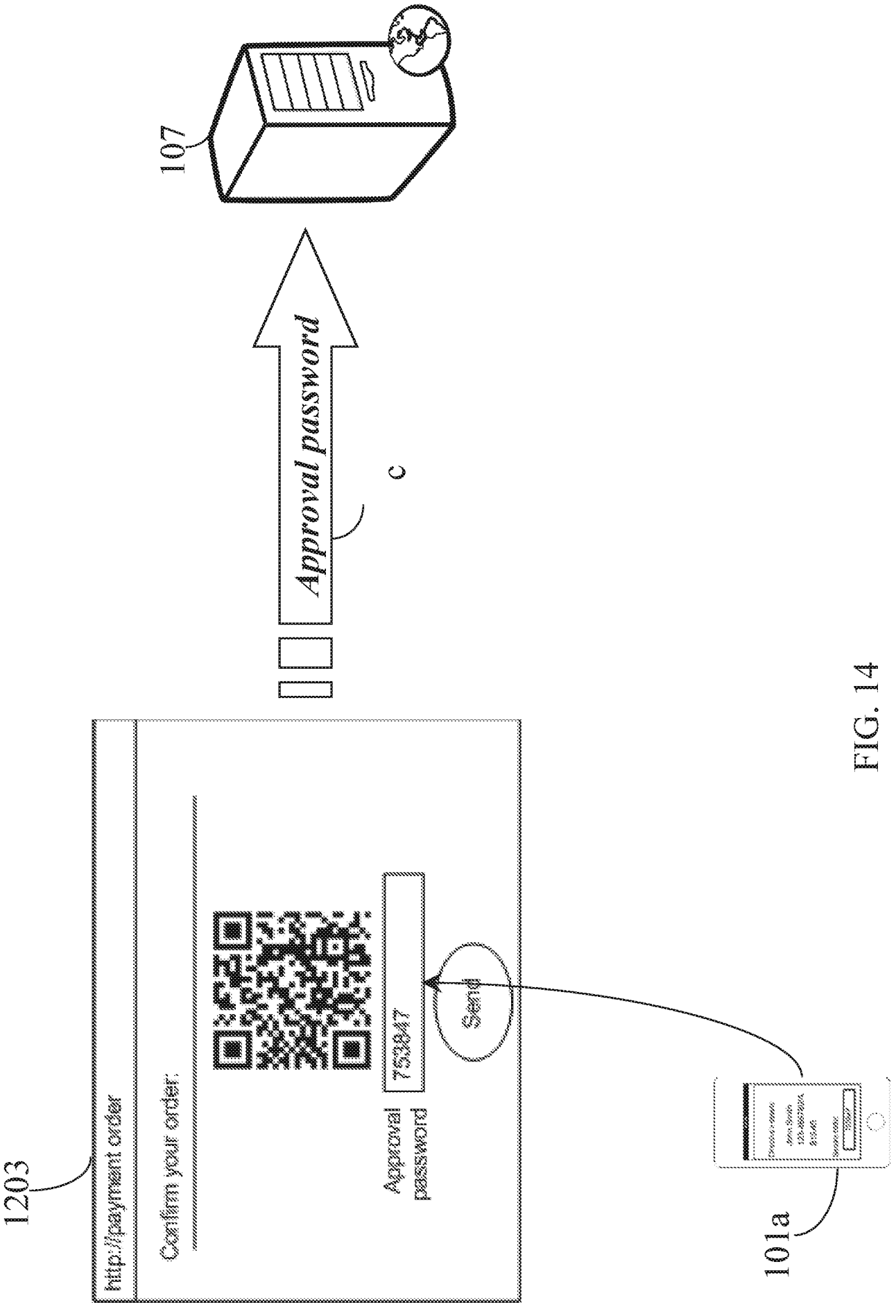
107
Approval password
c
1203
http://payment order
Confirm your order:
Approval password
763947
Send
101a

FIG. 14

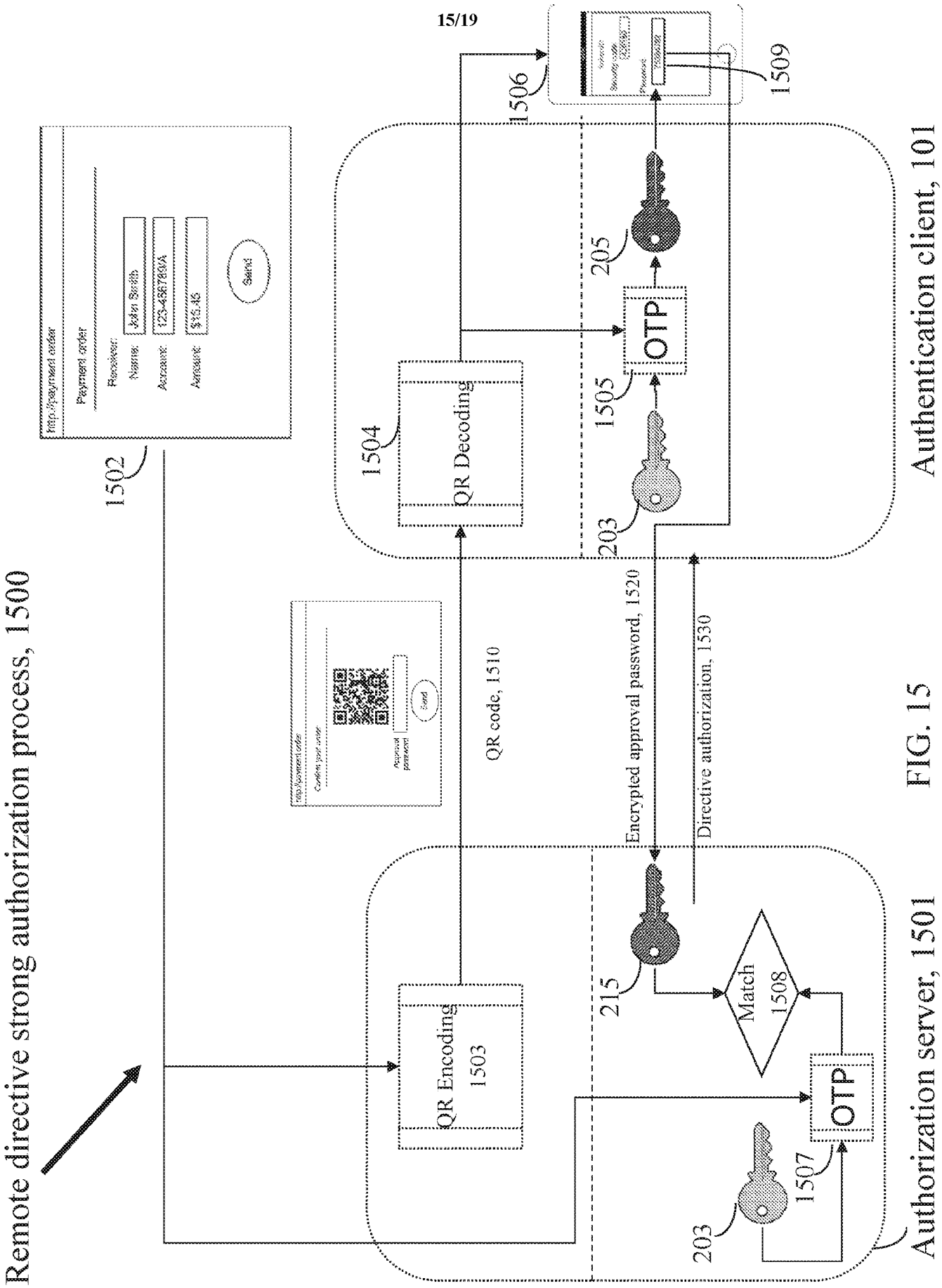
Remote directive strong authorization process, 1500
1502
1504
QR Decoding
1505
OTP
205
203
1506
1509
Authentication client, 1501
QR code, 1510
Encrypted approval password, 1520
Directive authorization, 1530
QR Encoding
1503
215
Match
1508
OTP
1507
203
Authorization server, 1501

FIG. 15

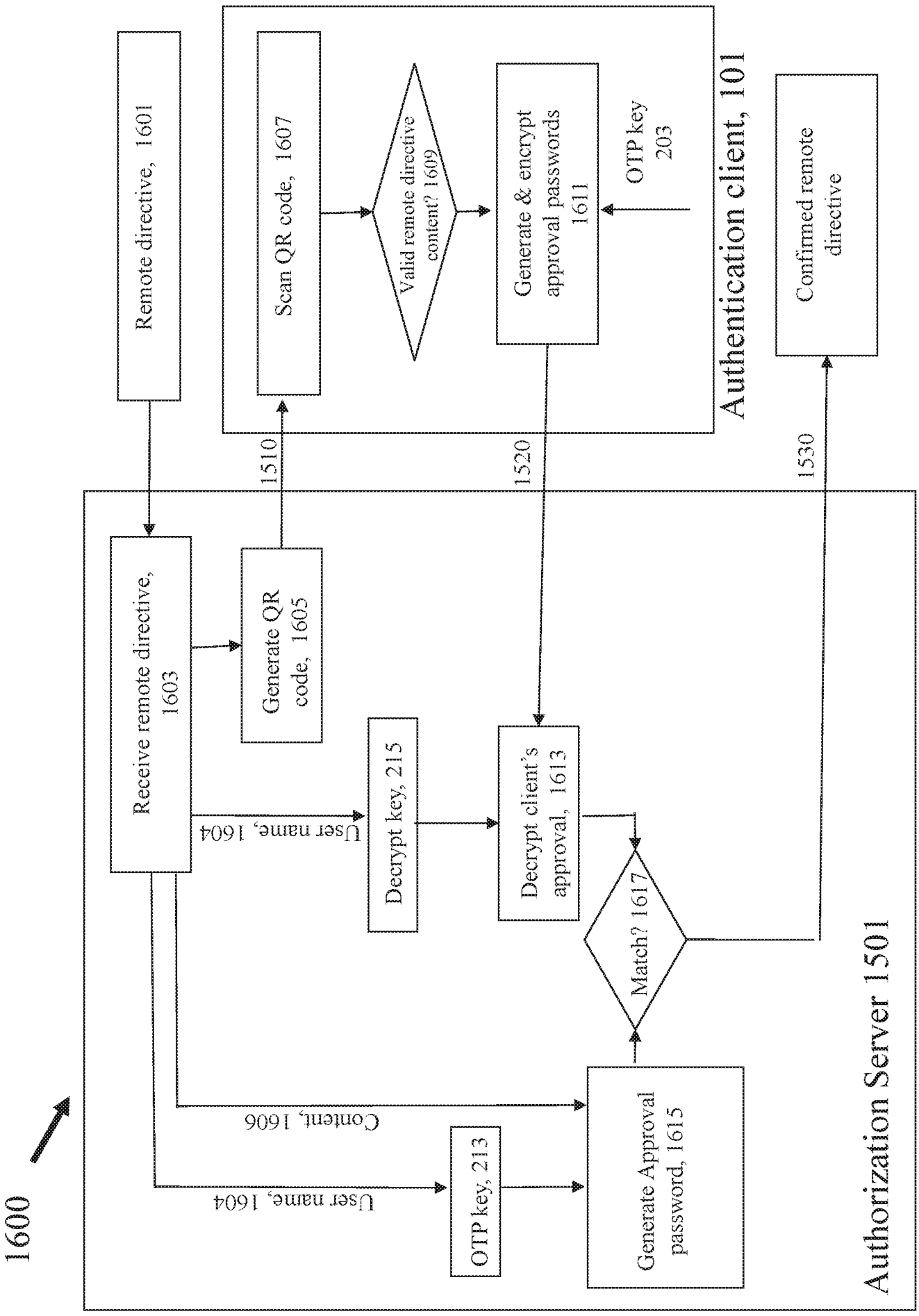
1600
Authorization Server 1501
Receive remote directive, 1603
Generate QR code, 1605
Decrypt key, 215
Decrypt client's approval, 1613
Match? 1617
Generate Approval password, 1615
OTP key, 213
User name, 1604
Content, 1606
User name, 1604
1510
1520
1530
Remote directive, 1601
Authentication client, 101
Scan QR code, 1607
Valid remote directive content? 1609
Generate & encrypt approval passwords 1611
OTP key 203
Confirmed remote directive

FIG. 16

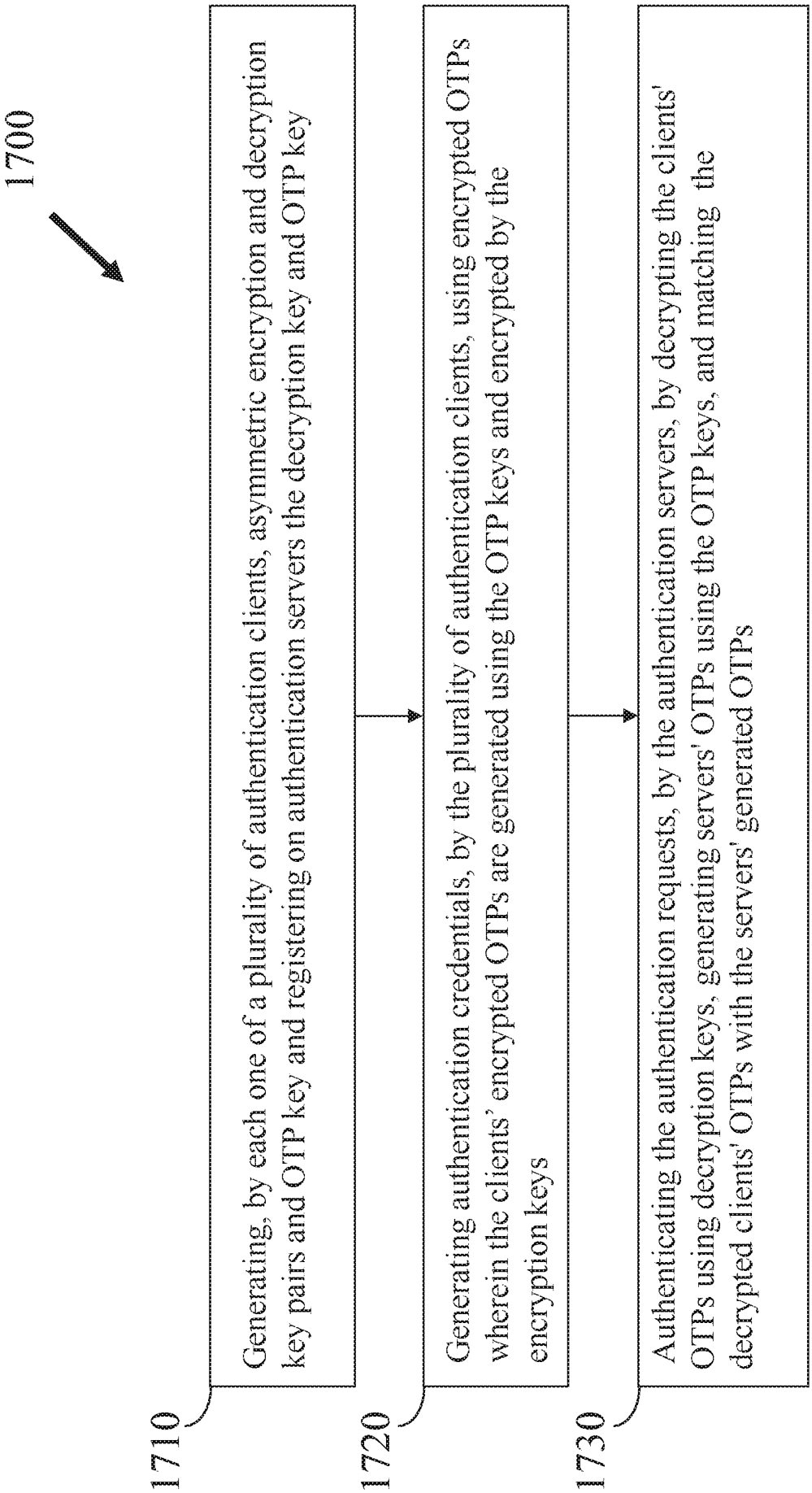
1700
1710
Generating, by each one of a plurality of authentication clients, asymmetric encryption and decryption key pairs and OTP key and registering on authentication servers the decryption key and OTP key
1720
Generating authentication credentials, by the plurality of authentication clients, using encrypted OTPs wherein the clients' encrypted OTPs are generated using the OTP keys and encrypted by the encryption keys
1730
Authenticating the authentication requests, by the authentication servers, by decrypting the clients' OTPs using decryption keys, generating servers' OTPs using the OTP keys, and matching the decrypted clients' OTPs with the servers' generated OTPs

FIG. 17

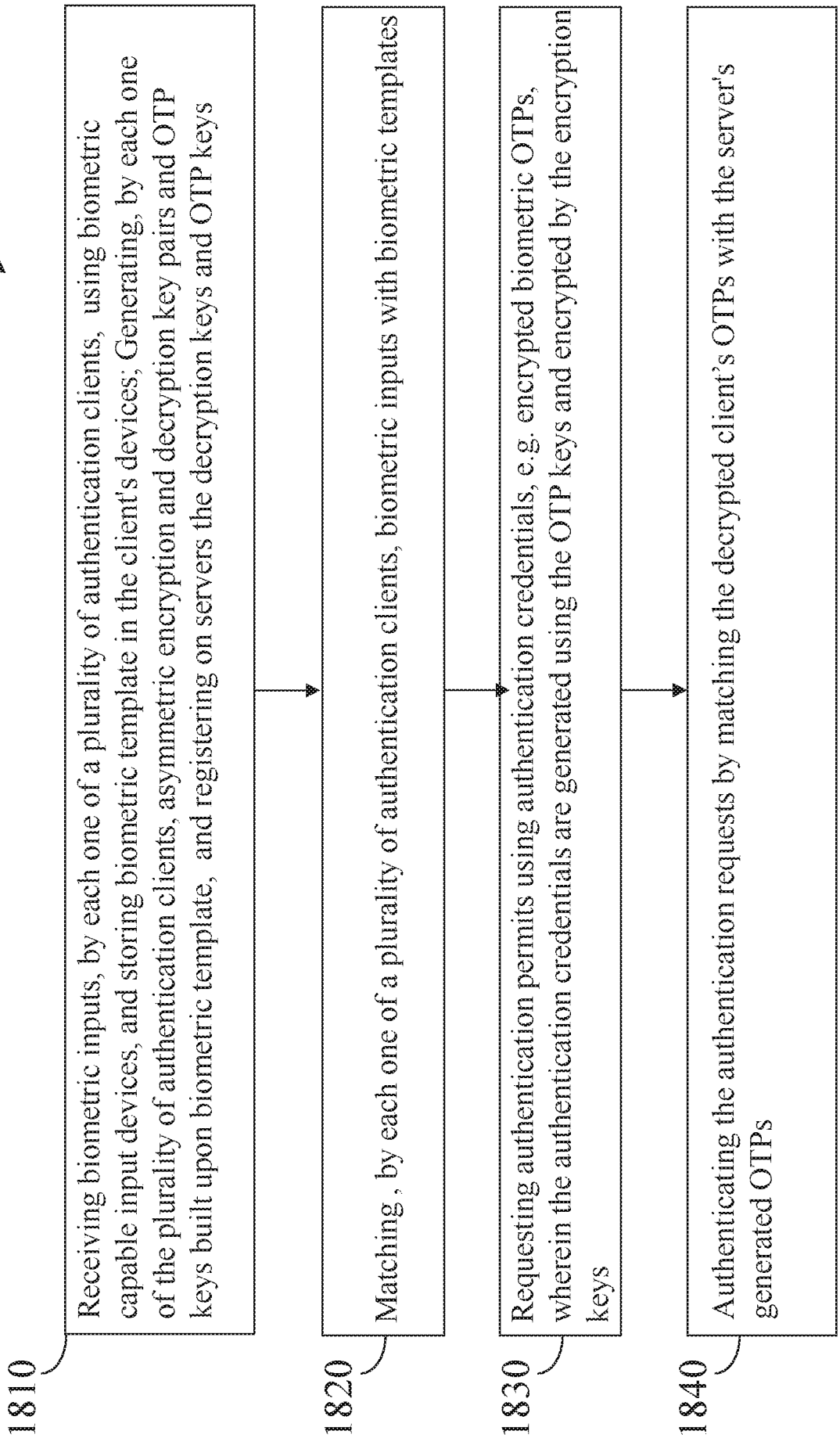
1800
1810
Receiving biometric inputs, by each one of a plurality of authentication clients, using biometric capable input devices, and storing biometric template in the client's devices; Generating, by each one of the plurality of authentication clients, asymmetric encryption and decryption key pairs and OTP keys built upon biometric template, and registering on servers the decryption keys and OTP keys
1820
Matching , by each one of a plurality of authentication clients, biometric inputs with biometric templates
1830
Requesting authentication permits using authentication credentials, e.g. encrypted biometric OTPs, wherein the authentication credentials are generated using the OTP keys and encrypted by the encryption keys
1840
Authenticating the authentication requests by matching the decrypted client's OTPs with the server's generated OTPs

FIG. 18

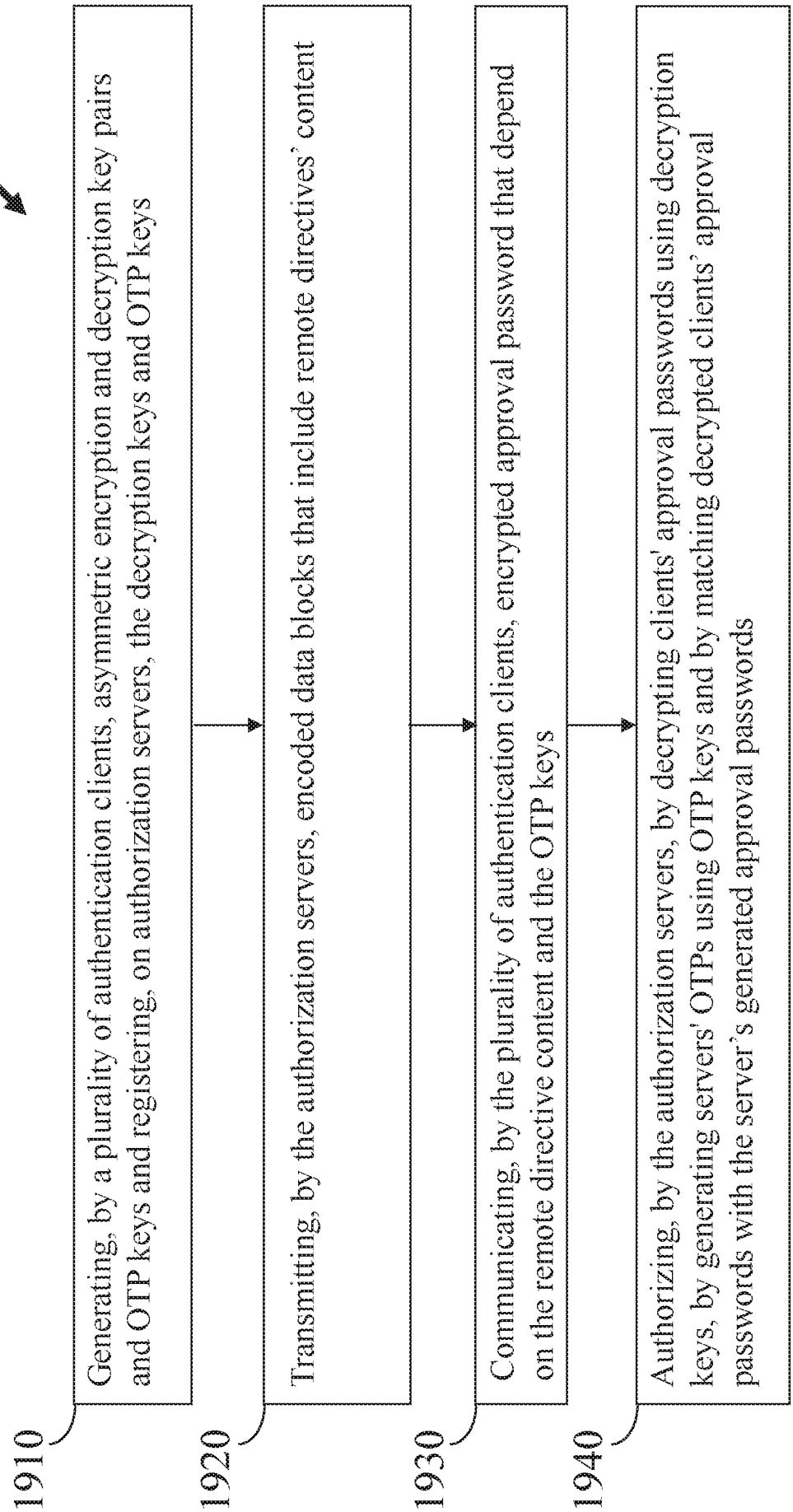
1900
1910
Generating, by a plurality of authentication clients, asymmetric encryption and decryption key pairs and OTP keys and registering, on authorization servers, the decryption keys and OTP keys
1920
Transmitting, by the authorization servers, encoded data blocks that include remote directives' content
1930
Communicating, by the plurality of authentication clients, encrypted approval password that depend on the remote directive content and the OTP keys
1940
Authorizing, by the authorization servers, by decrypting clients' approval passwords using decryption keys, by generating servers' OTPs using OTP keys and by matching decrypted clients' approval passwords with the server's generated approval passwords

FIG. 19

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2014/050263

A. CLASSIFICATION OF SUBJECT MATTER

IPC (2014.01) G06F 21/31, G06F 21/00, G06F 21/30, G06F 7/04, H04L 9/32

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 (2014.01) G06F 21/31, G06F 21/00, G06F 21/30, G06F 7/04, H04L 9/32

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Databases consulted: Esp@cenet, Google Patents, Google Scholar, FamPat database
Search terms used: ASYMMETRIC AUTHENTICATION OTP ONE-TIME-PASSWORD ONE TIME PASSWORD ENCRYPT BIOMETRIC QR

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005050330 A1 AGAM et al. 03 Mar 2005 (2005/03/03) The whole document	1,2,4-6,15,16
Y	The whole document	3,7-14
X	US 2012204245 A1 TING et al 09 Aug 2012 (2012/08/09) Abstract, paragraphs 0006,0027-0038, 0040	17,18
Y	The whole document	3,7-10
X	US 2012240204 A1 BHATNAGAR et al. 20 Sep 2012 (2012/09/20) Abstract, paragraphs 0008-0009, 0021-0023, 0040-0053, 0060	19-21
Y	The whole document	11-14

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

[X] See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 Jul 2014	09 Jul 2014
Name and mailing address of the ISA: Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Facsimile No. 972-2-5651616	Authorized officer PLACHINTA Ekaterina Telephone No. 972-2-5651740

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2014/050263

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2002144128 A1 RAHMAN et al. 03 Oct 2002 (2002/10/03) Abstract, paragraphs 0016, 0024	8-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IL2014/050263

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
US 2005050330 A1	03 Mar 2005	US 2005050330 A1	03 Mar 2005
		CN 1864364 A	15 Nov 2006
		EP 1658695 A2	24 May 2006
		IL 173946 D0	05 Jul 2006
		JP 2007503646 A	22 Feb 2007
		RU 2006109501 A	20 Oct 2007
		RU 2346396 C2	10 Feb 2009
		WO 2005022288 A2	10 Mar 2005
		WO 2005022288 A3	19 May 2005
US 2012204245 A1	09 Aug 2012	US 2012204245 A1	09 Aug 2012
		US 8683562 B2	25 Mar 2014
US 2002144128 A1	03 Oct 2002	US 2002144128 A1	03 Oct 2002
		US 7114080 B2	26 Sep 2006
US 2012240204 A1	20 Sep 2012	US 2012240204 A1	20 Sep 2012
		US 8763097 B2	24 Jun 2014