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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 April 2018 (12.04.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/065820 A1

(51) International Patent Classification:
G06F 21/36 (2013.01) *G06F 21/34* (2013.01)
G06F 21/42 (2013.01) *H04W 12/06* (2009.01)
G06Q 20/32 (2012.01) *G06Q 20/10* (2012.01)
H04L 29/06 (2006.01) *G06K 7/14* (2006.01)

(21) International Application Number:
PCT/IB2017/001362

(22) International Filing Date:
04 October 2017 (04.10.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/404,130 04 October 2016 (04.10.2016) US
62/411,107 21 October 2016 (21.10.2016) US

(71) Applicant: **ASSA ABLOY AB** [SE/SE]; Klarabergsviadukten 90, SE-111 64 Stockholm (SE).

(72) Inventors: **HOLLAND, James, William**; Fernside, Crookhill, Braishfield, Romsey SO51 (GB). **GUYOMARC'H, Francois-eric Michel**; 4 Rue Arboras, 34800 Clermont l'herault (FR). **KHAN, Milan**; Unit 3 Cae Gwyrdd, Green Meadow Springs Business Park, Wales CF15 7AB (GB). **WATTLES, Caleb**; 11 Rue De Champ De Mars, Paris (FR).

(74) Agent: **MUIRHEAD, Donald W.**; Muirhead And Saturnelli, Llc, 200 Friberd Parkway, Suite 1001, Westborough MA 01581 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,

(54) Title: MULTI FACTOR AUTHENTICATION USING DIFFERENT DEVICES

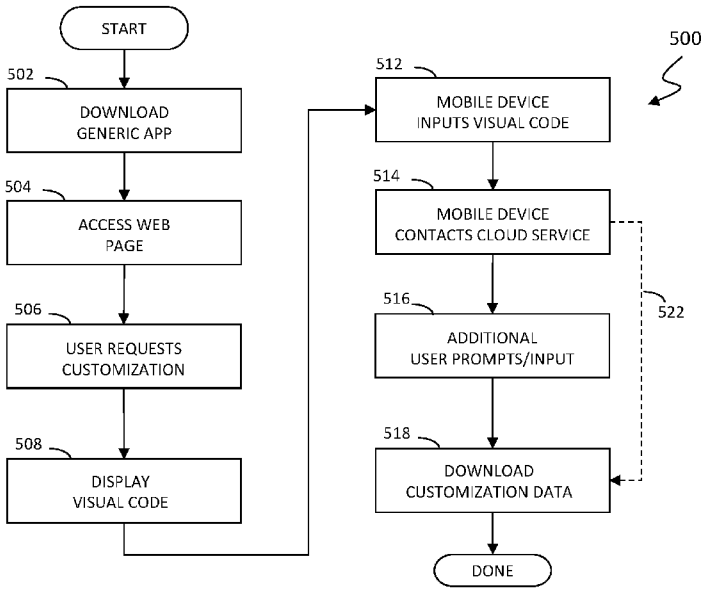


FIG. 5

(57) Abstract: Customizing an application on a mobile device includes storing at least a portion of customization data in a customization server that is independent of the mobile device, a user of the mobile device accessing the customization server independently of the mobile device, receiving authorization data from the customization server that enables the mobile device to securely receive customization data from the customization server, and the mobile device using the authorization data to cause the customization server to provide the customization data to the mobile device. The authorization data may be provided by postal message, email message, an SMS text message, and/or a visual code provided on a screen of a computer used to access the customization server. The user may use a computer to provide credential information to access the customization server. Customizing the application may allow the mobile device to access a user service on behalf of the user.

WO 2018/065820 A1

[Continued on next page]

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))*

— *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))*

MULTI FACTOR AUTHENTICATION USING DIFFERENT DEVICES

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to U.S. Provisional Patent Application No. 62/404,130 filed on October 4, 2016 titled CUSTOMIZING MOBILE APPLICATIONS and to U.S. Provisional Patent Application No. 62/411,107 filed on October 21, 2016 titled CUSTOMIZING MOBILE APPLICATIONS, both of which are incorporated by reference herein.

TECHNICAL FIELD

This application relates to the field of customizing applications and more particularly to the field of customizing mobile applications to facilitate security, use and appearance.

BACKGROUND OF THE INVENTION

In many areas of today's mobile oriented, modern life, consumers interact with service providers through the use of mobile applications running on mobile devices (e.g. smart phones). These service providers include organizations such as banks and other financial institutions, retailers, healthcare providers and media content providers etc. These providers may deliver their services through a custom corporate mobile application that is branded with their corporate identity and personalized/customized for their users (device owners).

In many cases, it is desirable to personalize a custom corporate mobile application running on a mobile device of a user. For example, a user may have a mobile banking application that displays account balances and transactions, transfers money, etc. For security reasons, the bank may not want to allow any mobile device to access any account or to enable all transactions for a given account via mobile applications. In some cases, a banking organization may have two or more versions of a custom corporate application. Premium bank customers, or business banking customers may have their own custom mobile application that provides features above and beyond their standard offering.

Many service providers within the same industry have similar needs on their mobile applications, e.g. show bank account information; capture user registration details etc. One common identified need that service providers have is the need to be able to identify and verify their users and to let the users approve actions within the mobile applications, connected to the services offerred by the service providers. Every service provider could

implement a custom process for approving an action within their mobile application, e.g. "Are you sure you wish to complete the checkout?" A service provider can spend considerable efforts in the design and building of such workflows into their mobile applications.

A mechanism for securely personalizing/customizing each instance of a mobile application, for each user, may require physical access to each mobile device. For example, each user of a mobile banking application may need to visit a branch of the bank to obtain customization. This may be a secure process, but in many cases, it may be impractical or, at the very least, relatively expensive for the bank to implement (because of extra banking personnel needed) and likely to be very inconvenient for the customers (waiting for someone to be available to help, having access only during certain hours, etc.).

An alternative way to get personalized/customized information onto a users mobile devices is to point end users to an appropriate custom corporate mobile application for their needs, and allow the users to personalize/customize the mobile application remotely, over-the-air. This mechanism could remotely provide users with personalization/customization data, e.g. through wireless networks. However, providing personalization/customization data remotely can raise security issues (i.e. user B intercepts and loads remote personalization/ customization information meant for user A) and can cause difficulties for users, such as when a user incorrectly loads personalization/customization information for one device on to another device. Thus custom corporate mobile applications may be difficult to write and may require significant expertise in the security field.

Accordingly, it is desirable to provide a mechanism for allowing a user to personalize/customize a mobile application remotely in a way that is secure and does not involve participation by personnel at a corresponding organization and/or does not require development of corporate custom applications.

SUMMARY OF THE INVENTION

According to the system described herein, customizing an application on a mobile device includes storing at least a portion of customization data in a customization server that is independent of the mobile device, a user of the mobile device accessing the customization server independently of the mobile device, receiving authorization data from the customization server that enables the mobile device to securely receive customization data

from the customization server, and the mobile device using the authorization data to cause the customization server to provide the customization data to the mobile device. The authorization data may be provided by postal message, email message, an SMS text message, and/or a visual code provided on a screen of a computer used to access the customization server. The user may use a computer to provide credential information to access the customization server. The authorization data may be provided by the visual code on a screen of the computer and the mobile device may input the visual code using a camera of the mobile device. Customizing the application may allow the mobile device to access a user service on behalf of the user. The user service may be provided by the customization server. The customization data may include a secret key that allows the mobile device to access the user service. The user service may be banking. A template may be used to populate the customization data. Certificate pinning may be used to require that the mobile device only communiation with predetermined customization servers.

According further to the system described herein, a non-transitory computer-readable medium contains software that customizes an application on a mobile device. The software includes executable code that stores at least a portion of customization data in a customization server that is independent of the mobile device, wherein a user of the mobile device accesses the customization server independently of the mobile device, executable code that receives authorization data from the customization server that enables the mobile device to securely receive customization data from the customization server, and executable code that enables the mobile device to use use the authorization data to cause the customization server to provide the customization data to the mobile device. The authorization data may be provided by postal message, email message, an SMS text message, and/or a visual code provided on a screen of a computer used to access the customization server. The user may use a computer to provide credential information to access the customization server. The authorization data may be provided by the visual code on a screen of the computer and the mobile device may input the visual code using a camera of the mobile device. Executable code that customizes the application may allow the mobile device to access a user service on behalf of the user. The user service may be provided by the customization server. The customization data may include a secret key that allows the mobile device to access the user service. The user service may be banking. A template may be used to populate the customization data. Certificate pinning may be used to require that the mobile device only communiation with predetermined

customization servers.

A customization server is created to enables service providers to customize (personalize) a mobile phone application of an end user without requiring programming capabilities by the service provider. The customization server may provide an interface that addresses a need common to services provider organizations.

This customization server may allow a service provider to personalize and customize each instance of the mobile banking application in each mobile device of each user.

Each service provider organization may be able to customize the mobile application independently and autonomously of each other (i.e. have their own "containers" for personalization/customization data). A common customization server approvals process that is provided may tie each approval to the appropriate service provider (and it's container), such that, for example, approving a grocery checkout at Wal-Mart does not approve some other action at a different service provider.

Also, it is desirable for a service provider to be able to introduce trust into an untrusted mobile device in order to be able to electronically transact with the mobile device owner.

A mobile banking application may be customized and personalized to contain, for example, a secret key that verifies the particular user and allows encryption of communication with the bank. Other additions may include account information, indications of allowable transaction, and possibly information that changes the visual appearance of the app, such as branding information.

Note also that, in some cases, it may be useful to confirm that a user has physical possession of a mobile device prior to customizing the device (i.e. for security and logistical reasons). This device may be a device that is preregistered with the service provider.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the system described herein are explained with reference to the several figures of the drawings, which are briefly described as follows.

FIG. 1 is a schematic illustration showing a computer and a mobile device having a generic app that is being customized according to an embodiment of the system described herein.

FIG. 2 is a schematic illustration showing a screen with a customization button thereon according to an embodiment of the system described herein.

FIG. 3 is a schematic illustration showing a screen with a visual code thereon according to an embodiment of the system described herein.

FIG. 4 is a schematic illustration showing a computer, a mobile device, and a service provider according to an embodiment of the system described herein.

FIG 5 is a flow diagram illustrating processing performed in connection with customizing a generic app on mobile device according to an embodiment of the system described herein.

FIG 6 is a flow diagram illustrating processing performed by a service provider in connection with receiving a request to customize a generic app on a mobile device according to an embodiment of the system described herein.

FIG. 7 is a schematic diagram showing a mobile device being customized using two separate service providers according to an embodiment of the system described herein.

FIG. 8 is a schematic diagram showing a mobile device running an app with a plurality of client containers according to an embodiment of the system described herein.

DETAILED DESCRIPTION OF VARIOUS EMBODIMENTS

The system described herein provides a secure and automated mechanism for a user to request and obtain custgomization data for a generic app on a mobile device.

Referring to FIG. 1, a diagram 100 shows a computer 102, such as a desktop or laptop computer, and a mobile device 104, such as a smartphone. The mobile device 104 may be an Android device or an IOS device and includes a generic app (not shown) that a user of the mobile device 104 desires to customize/personalize. Customizing an app on the mobile device 104 includes adding security information (e.g., user name and password, user digital certificate,

user secret key, etc.) that allows the app to have secure access to data. For example, if the app facilitates a user accessing and manipulating banking information for the user, then customizing the app may include providing specific information/credentials to the app that allows the user to securely access their account through the Internet. Providing customization to the app may also include providing configuration information specific to a particular user and/or group of users and, in some cases, modifying the way the app looks on the mobile device 104 so that, for example, customization may include "branding" where the app shows information for a particular brand/company on the mobile device 104. Customization may include pre-established preferences by the users, such as alert settings (when and how to send account alerts) and/or other types of personalization/customization.

The user causes the generic app on the mobile device 104 to be customized by capturing or entering initialization parameters provided by the service provider into the generic app to begin customization that is specific to the service provider and user. The initialization parameters may be communicated to the user by the service provider in a number of ways, including postal message, email message, SMS text message, QR code, verbally spoken string of characters, etc. In many cases, the user may initially contact a service provider independently of the mobile device 104 (e.g., without using the mobile device 104)

As an example, if the generic app is being customized/personalized for a particular bank, the user initially logs into a Web site for the particular bank using the computer 102. The user then retrieves the initialization parameters from the Web site for the particular bank. The initialization parameters may be displayed as a visual code (not shown in FIG. 1), such as a QR code, a bar code, or similar, on the screen of the computer 102. The user uses the mobile device 104 to capture the visual code using, for example, a camera of the mobile device 104. The mobile device 104 then decodes and uses the information provided by the visual code to customize the app on the mobile device 104, as described in more detail elsewhere herein.

Referring to FIG. 2, a screen 202 of a Web site for a service/business corresponding to the generic app being customized/personalized is provided in response to a user accessing the Web site. The screen 202 is used in connection with customizing the generic app on a mobile device of the user. In some cases, the screen 202 may only be available in response to the user providing appropriate credentials (e.g., user name and password). In other instances, the

screen 202 may be available without the user initially providing any credentials, although the user may be subsequently required to enter credential information (or similar) at some point prior to customization of the generic app.

The screen 202 may include a customize button 204 that the user actuates to customize the generic app on the mobile device of the user. In other instances, the button 204 may be replaced by a menu selection, a link (i.e., an HTML link), etc. The user actuates the button 204 (or similar) while the mobile device of the user is in proximity to the user. In an embodiment herein, the system may provide the user with a pre-determined amount of time to complete the customization process (described elsewhere herein) prior to timing out and requiring the user to begin the customization process again.

Referring to FIG. 3, a screen 302 is shown with a visual code 304 that is used by the user to customize/personalize the generic app on the mobile device of the user. The screen 302 and the visual code 304 are provided in response to the user actuating the button 204 (or similar). As described elsewhere herein, the user uses the mobile device to photograph the visual code 304 to provide information to the mobile device that is used for customization of a generic app provided thereon.

Referring to FIG. 4, a diagram 400 shows the computer 102 and the mobile device 104 coupled to a service provider 402. In an embodiment herein, the service provider 402 may be accessible from the World Wide Web, although in other embodiments, it is possible to make the service provider 402 not be accessible from the World Wide Web but, instead, have the service provider 402 be accessible only privately, either through a private network, via one or more direct connections, etc. Thus, connections from the computer 102 and the mobile device 104 to the service provider 402 represent accessing the service provider 402 through the World Wide Web, via a private network, direct connections, etc. The service provider 402 may include a business application, 410 (e.g. a banking application) and a server provider customization server 411 for customization.

The service provider customization server 411 stores data used for customization (personalization) of a generic app on a mobile device, including specific customization data, branding data, credential information, security information, such as keys, certificates, etc. In an embodiment herein, a template is used where the service provider modifies the template to

include visual items such as a service label, a service background color, a logo (bitmap image), a foreground color, etc. The customization server 411 also provides processing for determining whether and which customization data to provide based on which "container" data is associated with as well as possibly security processing to confirm security information used in connection with requesting and authorizing customization of a generic app. As described in more detail elsewhere herein, once the mobile device 104 has photographed (or similar) the visual code on the computer 102, the mobile device 104 then communicates with the service provider customization server 411 to provide information corresponding to the visual code to the service provider 402 and to receive the customization information from the service provider customization server 411.

Referring to FIG. 5, a flow diagram 500 illustrates a user customizating a generic app on a mobile device. At a first step 502, the user downloads the generic app onto the mobile device. The step 502 may be performed using conventional app download mechanisms, such as, for example, accessing the generic app with an iOS device using the Apple app store. In some instances, it may also be possible to download the generic app onto the mobile device from the World Wide Web. Following the step 502 is a step 504 where the user accesses an appropriate Web page for retrieving the initialization parameters and customizing the generic app, as described elsewhere herein. In some embodiments, the user provides at least some credential information in order to be able to access the Web page or programmatic service at the step 504. In other cases (e.g. a two-step customization process) the user does not need to provide any credential information to access the Web page at the step 504, in which case the user may be required to provide credential information at a later time but prior to customization of the generic app. The user may access the Web page at the step 504 independently of the mobile device (e.g., without using the mobile device at all).

In some embodiments, the Web page accessed at the step 504 may be for a generic service provider that redirects the user to a different Web page for a specific service provider. For instances, a trusted broker may provide redirection to different, possibly unrelated, service providers. The user would access the Web page for the trusted broker at the step 504 and choose one of the service providers presented on the Web page. After making a choice, the user would then be redirected to a Web page for the specific service provider. In some cases,

certificate pinning may be used to enhance security by requiring that the mobile device only communicates with predetermined service providers/trusted brokers.

Following the step 504 is a step 506 where the user selects (actuates) customization at the Web page by, for example, clicking a button. Note that any other mechanism may be used to allow a user to actuate at the Web page to start customization of the generic app, such as menu selection, an HTML link, etc. The user may actuate the Web page at the step 506 independently of the mobile device (e.g., without using the mobile device at all). Following the step 506 is a step 508 where a visual code is displayed on a screen of the computer used to access the Web page, as described elsewhere herein. Following the step 508 is a step 512 where the user photographs (or similar) the visual code. As discussed elsewhere herein, the visual code is an encoding of the initialization parameters and includes information that is used to identify and authenticate the request e.g. a one-time password value (or similar) to provide security.

Following the step 512 is a step 514 where the mobile device connects with the service provider customization server (discussed elsewhere herein) that provides the customization information for the mobile device. Connecting with the service provider customization server at the step 514 includes the mobile device providing the service provider customization server with some or all of the information that the mobile device received from the initialization parameters (which may be presented as a visual code) as well as possibly other information, such as a serial number, user ID, etc. associated with the mobile device. Following the step 514 is a step 516 where the user is prompted to enter additional information/credentials. In some cases, the service provider customization server may require additional verification information from the user (e.g., a password, a physiological or behavioral characteristic such as a fingerprint biometric , voice recognition, facial recognition, etc.). It is also possible for the additional information to include additional configuration information that can be applied in the app customization, such as asking the user for a nearest/preferred branch of a particular bank. Following the step 516, control transfers to a step 518 where the mobile device downloads the customization data from the service provider customization server. Following the step 518, processing is complete.

In some embodiments, it may not be necessary/desirable to request that the user provide additional information at the step 516 after the mobile device connects to the service provider customization server at the step 514. For example, in some embodiments, it is possible to have the user provide all necessary/desirable information for credentials, security, configuration, etc. in connection with accessing the Web page at the step 504, discussed above. In such a case, it may be possible to forgo the step 516 altogether, which is indicated by an alternative path 522 that provides that the step 518 immediately follows the step 514.

Referring to FIG. 6, a flow diagram 600 illustrates steps performed at the service provider customization server 411 (not shown in FIG. 6) in connection with servicing a request for customization of a mobile device. Processing begins at a first step 602 where the service provider receives a request for customization. Following the step 602 is a test step 604 where the service provider customization server determines if the request and/or user are authorized for customization. In some cases, the test at the step 604 may turn, at least in part, on the circumstances of the request. For example, for a U.S. bank, requests from computers that are located outside of North America may not be authorized so as to provide protection against fraud. The test at the step 604 may also turn on an identity of the user making the request (e.g., bank customer or not) and/or the particular mobile device (e.g., device with particular minimum technical capability, pre-registered device, etc.).

If it is determined at the test step 604 that the user/device is not authorized, then processing is complete and the service provider customization server takes no further steps to provide customization for the mobile device of the user. Otherwise, if the user/device is authorized, control transfers from the test step 604 to a step 606 where the service provider causes the initialization parameters (e.g., the QR code 304, discussed above) to be displayed. Following the step 606 is a step 608 where the service provider customization server receives a communication from the mobile device following the mobile device capturing the initialization parameters (described elsewhere herein). The communication from the mobile device may include information extracted from the initialization parameters, such as the service/application, user identity, a one time password (or similar), and possibly other data, that allows mobile and server to establish a shared key.

Following the step 608 is a step 612 where the system matches the information received at the step 608 with information already stored at the service provider. For example, if the mobile device is being customized for a bank app, processing at the step 612 may include matching the user with specific user accounts and perhaps also with a pre-determined list of allowed transactions and limits. Other processing at the step 612 may include matching the particular device with particular capabilities. For example, different customization capabilities may be provided depending on whether the mobile device is a tablet or a smartphone. Note also that additional checks may be performed at the step 612, including, for example, determining if the specific mobile device is authorized (not on a black list), determining if a phone number for the mobile device matches a known phone number for the user, is the location of the device proximate to a known address/location for the user, has the device been used previously by the user; whether the device is jaibroken or rooted; whether the device contains a secure element (smart card or TEE); whether the device has a certain OS version etc. In some instances, if one or more of the additional check are failed, customization may be terminated, which is not shown in FIG. 6.

Following the step 612 is a test step 614 where it is determined if the user/device will be prompted for additional data. For example, once a specific mobile device has been identified (e.g., by serial number), the service provider may prompt the device for an expected value, such as a nonce encrypted with a secret key, to confirm the authenticity of the device. Other prompted information may include, for example, querying the user for a favorite/closest bank branch. If it is determined at the test step 614 that additional data is needed from the user and/or the mobile device, then control transfers from the test step 614 to a step 616, where the additional data is obtained. Note that, in some cases, the additional data obtained at the step 616 includes security data and failure to provide appropriate data (e.g., a digital certificate, a user password, etc.) could result in termination of the customization process, which is not shown in FIG. 6.

Following the step 616 or following the step 614 if prompting is not performed, is a step 618 where the service provider sends customization data to the mobile device. In some instances, the customization data may be specific for a single user. In other cases, the customization data may correspond to data provided to a particular group to which the user belongs (e.g., Massachusetts banking customers). The customization data may include, for

example, one time password configuration data (i.e., a seed), a private key generated at the service provider customization server 411, a private key and a digital certificate containing the corresponding public key, a proprietary identity, such as a SEOS key, etc. The customization data is optionally protected for integrity and confidentiality using shared keys established in a previous step of the process. The customization data could also include graphical personalization/ customization, such as logos, icons, and textual changes to titles, buttons, menus, etc. Following the step 618, processing is complete.

Referring to FIG. 7, a diagram 700 illustrates the mobile device 104 having an app 702 that includes a plurality of client containers 704-706 and executable code 708. Each of the client containers 704-706 includes separate customization for different services. Some or all of the client containers 704-706 may be customized by different service providers. Thus, the app 702 is essentially customized from different, possibly unrelated, services which are possibly from different cloud services. The diagram 700 shows the client containers 704, 705 being customized by a first cloud service 402' having a first set of customization data 704' for the client container 704 and a second set of customization data 705' for the client container 705. The client container 706 is customized by a second cloud service 402'' having a set of customization data 706'. Note that the executable code 708 of the app 702 is not effected by the client containers 704-706 or the cloud services 402', 402''. In an embodiment herein, the executable code 702 may be generic to all services and customizations, but the user is presented with what looks like a different app depending upon the particular customization. Thus, for example, the user could download a generic banking app that could be separatly customized for different, unrelated, banks so that the user has a different app experience for each of the banks even though the user is running the same generic executable code for all the banks.

Different keys are used for transmission between the client containers 704-706 and the sets of customization data 704'-706'. In an embodiment herein, keys used by each of the containers 704-706 and a corresponding one of the sets of customization data 704'-706' are exclusive and known only to communicating entities. Thus, for example, the keys (or single symmetric key) used by the client container 704 and in connection with the customization data 704' are known only to the first cloud service 402' and the client container 704 and are not interchangeable or replaceable with any other keys. This prevents another cloud service, such

as the cloud service 402'', from improperly updating an unrelated client container, such as the client container 704.

In some embodiments, the mobile device 104 communicates with a single cloud service 708 which passes communcation to an appropriate one of the cloud services 402', 402''. Thus, the mobile device 104 does not need to have direct access to the cloud services 402', 402'' but, instead, relies on the cloud service 708 to relay communications therefor. In an embodiment herein, the cloud servive 708 does not have access to data in the client containers 704-706 and does not have access to any of the keys used to encrypt data communicated between the mobile device 104 and the cloud services 402', 402''. Thus, even though the cloud service 708 relays data, the cloud service 708 does not have access to any of the data being relayed.

Referring to FIG. 8, a diagram 800 shows a mobile device 802 running an app 804 having a plurality of client containers. As discussed elsewhere herein, each of the client containers of the app provide customization of different, possibly unrelated, services. Some or all of the client containers may be customized by different cloud services. Thus, a user may run the app 804 on the mobile device 802 and select from among the client containers that have been customized, as described elsewhere herein.

The system described herein may be provided without the need for development of custom application code.

Various embodiments discussed herein may be combined with each other in appropriate combinations in connection with the system described herein. Additionally, in some instances, the order of steps in the flowcharts or flow diagrams may be modified, where appropriate. Further, various aspects of the system described herein may be implemented using software, hardware, a combination of software and hardware and/or other computer-implemented modules or devices having the described features and performing the described functions. Software implementations of the system described herein may include executable code that is stored in a computer readable storage medium and executed by one or more processors. The computer readable storage medium may include a computer hard drive, ROM, RAM, flash memory, portable computer storage media such as a CD-ROM, a DVD-ROM, a flash drive and/or other drive with, for example, a universal serial bus (USB) interface, and/or any other appropriate tangible storage medium or computer memory on which executable code

may be stored and executed by a processor. The system described herein may be used in connection with any appropriate operating system.

Other embodiments of the invention will be apparent to those skilled in the art from a consideration of the specification or practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only.

What is claimed is:

1. A method of customizing an application on a mobile device, comprising:

storing at least a portion of customization data in a customization server that is independent of the mobile device;

a user of the mobile device accessing the customization server independently of the mobile device;

receiving authorization data from the customization server that enables the mobile device to securely receive customization data from the customization server; and

the mobile device using the authorization data to cause the customization server to provide the customization data to the mobile device.

2. A method, according to claim 1, wherein the authorization data is provided by at least one of: postal message, email message, an SMS text message, or a visual code provided on a screen of a computer used to access the customization server.

3. A method, according to claim 2, wherein the user uses a computer to provide credential information to access the customization server.

4. A method, according to claim 3, wherein the authorization data is provided by the visual code on a screen of the computer and the mobile device inputs the visual code using a camera of the mobile device.

5. A method, according to claim 1, wherein customizing the application allows the mobile device to access a user service on behalf of the user.

6. A method, according to claim 5, wherein the user service is provided by the customization server.

7. A method, according to claim 5, wherein the customization data includes a secret key that allows the mobile device to access the user service.

8. A method, according to claim 5, wherein the user service is banking.

9. A method, according to claim 1, wherein a template is used to populate the customization data.

10. A method, according to claim 1, wherein certificate pinning is used to require that the mobile device only communiation with predetermined customization servers.

11. A non-transitory computer-readable medium containing software that customizes an application on a mobile device, the software comprising:

executable code that stores at least a portion of customization data in a customization server that is independent of the mobile device, wherein a user of the mobile device accesses the customization server independently of the mobile device;

executable code that receives authorization data from the customization server that enables the mobile device to securely receive customization data from the customization server; and

executable code that enables the mobile device to use use the authorization data to cause the customization server to provide the customization data to the mobile device.

12. A non-transitory computer-readable medium, according to claim 11, wherein the authorization data is provided by at least one of: postal message, email message, an SMS text message, or a visual code provided on a screen of a computer used to access the customization server.

13. A non-transitory computer-readable medium, according to claim 12, wherein the user uses a computer to provide credential information to access the customization server.

14. A non-transitory computer-readable medium, according to claim 13, wherein the authorization data is provided by the visual code on a screen of the computer and the mobile device inputs the visual code using a camera of the mobile device.

15. A non-transitory computer-readable medium, according to claim 11, wherein executable code that customizes the application allows the mobile device to access a user service on behalf of the user.

16. A non-transitory computer-readable medium, according to claim 15, wherein the user service is provided by the customization server.

17. A non-transitory computer-readable medium, according to claim 15, wherein the customization data includes a secret key that allows the mobile device to access the user service.

18. A non-transitory computer-readable medium, according to claim 15, wherein the user service is banking.

19. A non-transitory computer-readable medium, according to claim 11, wherein a template is used to populate the customization data.

20. A non-transitory computer-readable medium, according to claim 11, wherein certificate pinning is used to require that the mobile device only communiation with predetermined customization servers.

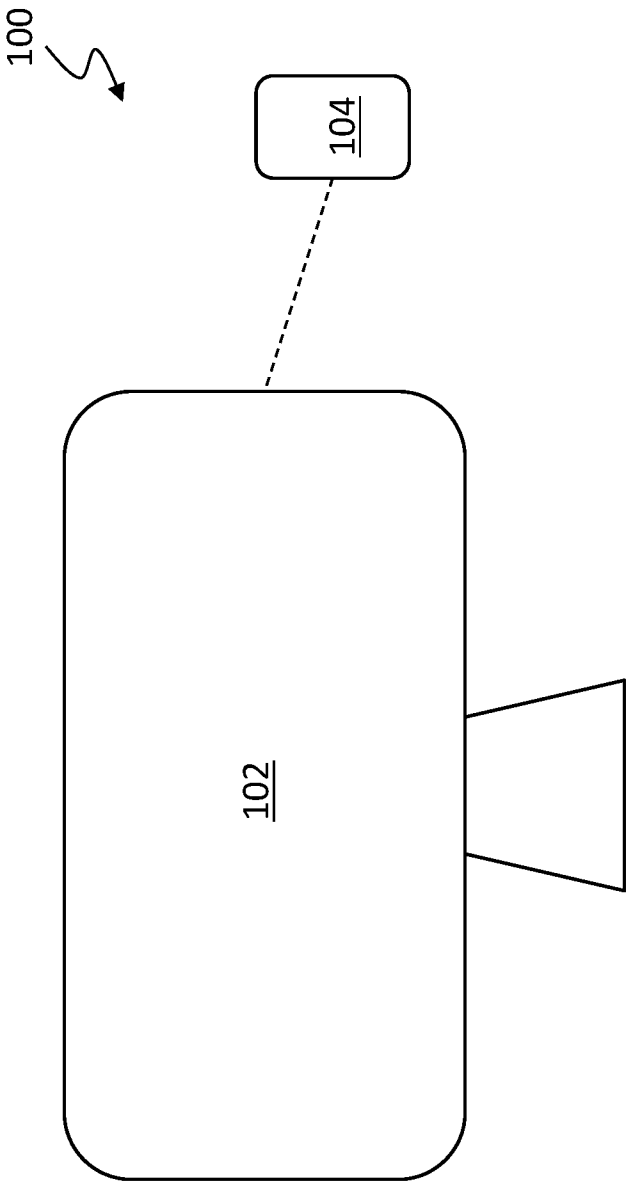


FIG. 1

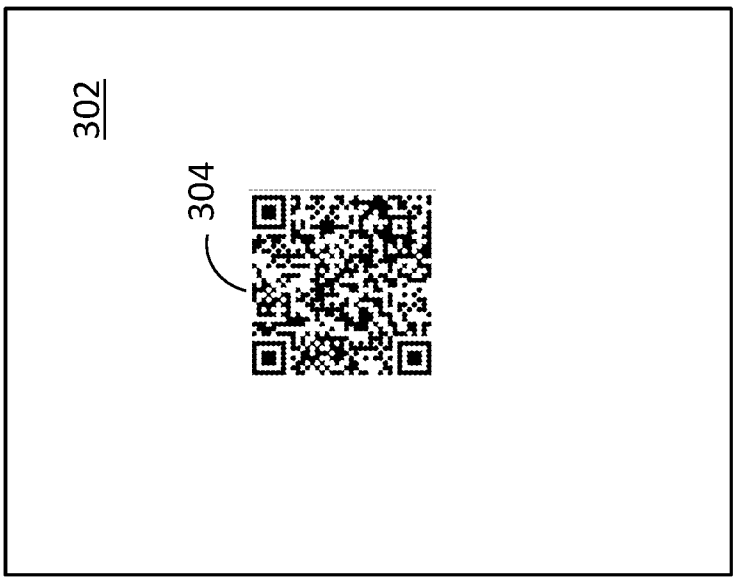


FIG. 3

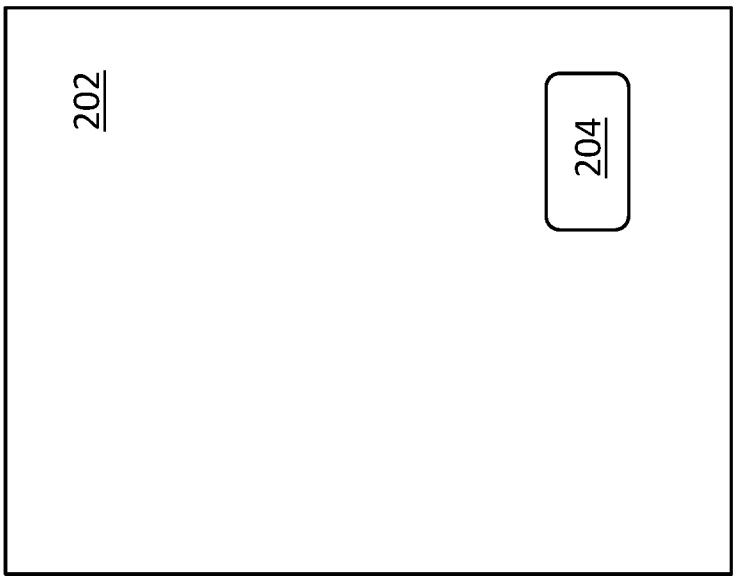


FIG. 2

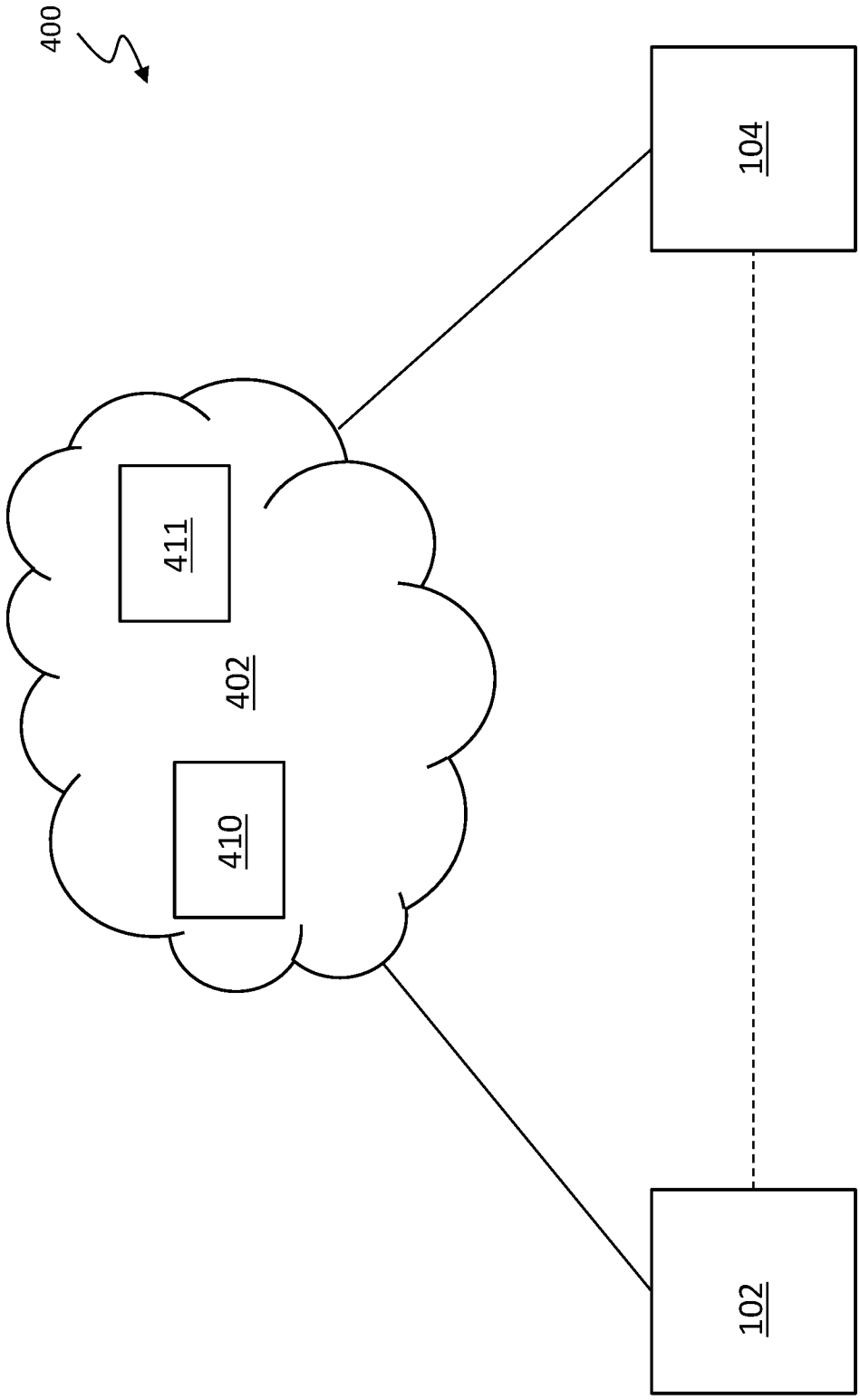


FIG. 4

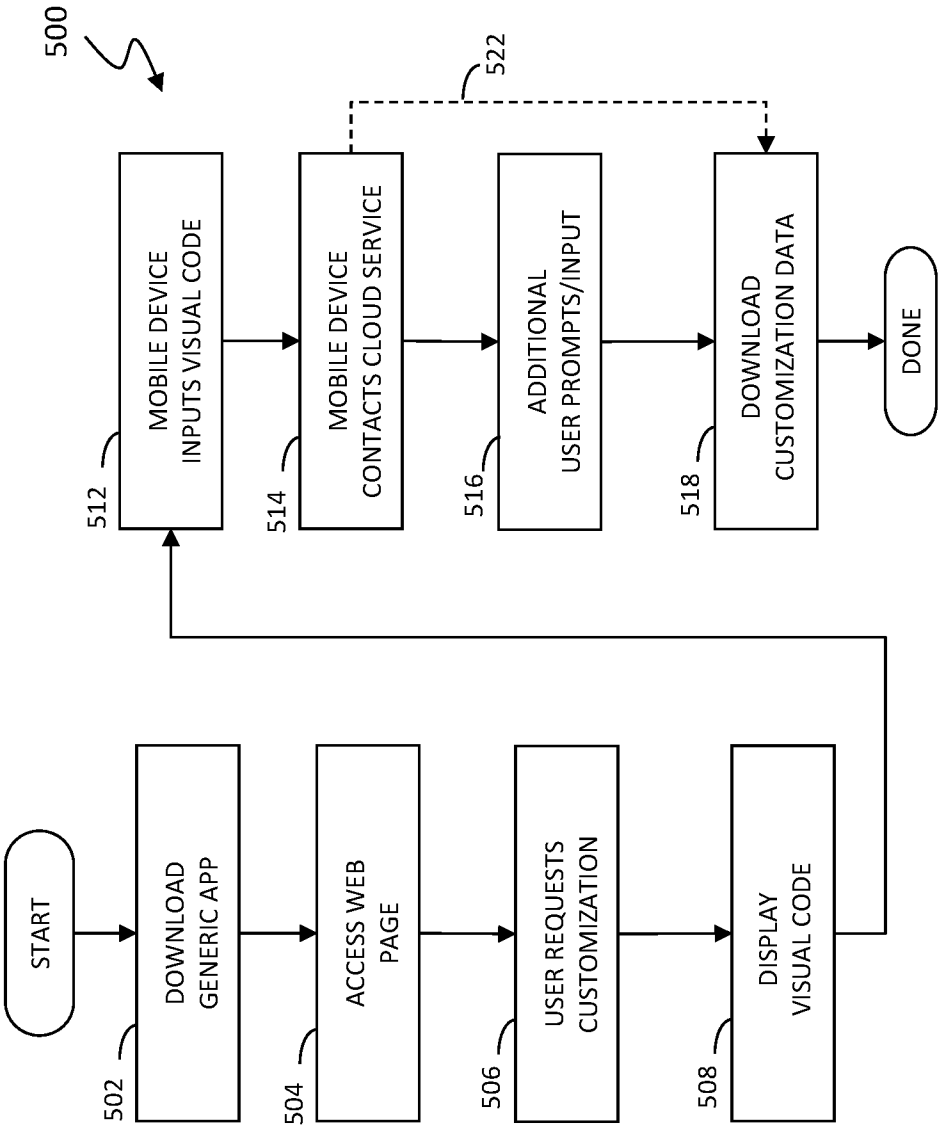

500
522
START
DOWNLOAD GENERIC APP
ACCESS WEB PAGE
USER REQUESTS CUSTOMIZATION
DISPLAY VISUAL CODE
MOBILE DEVICE INPUTS VISUAL CODE
MOBILE DEVICE CONTACTS CLOUD SERVICE
ADDITIONAL USER PROMPTS/INPUT
DOWNLOAD CUSTOMIZATION DATA
DONE
502
504
506
508
512
514
516
518

FIG. 5

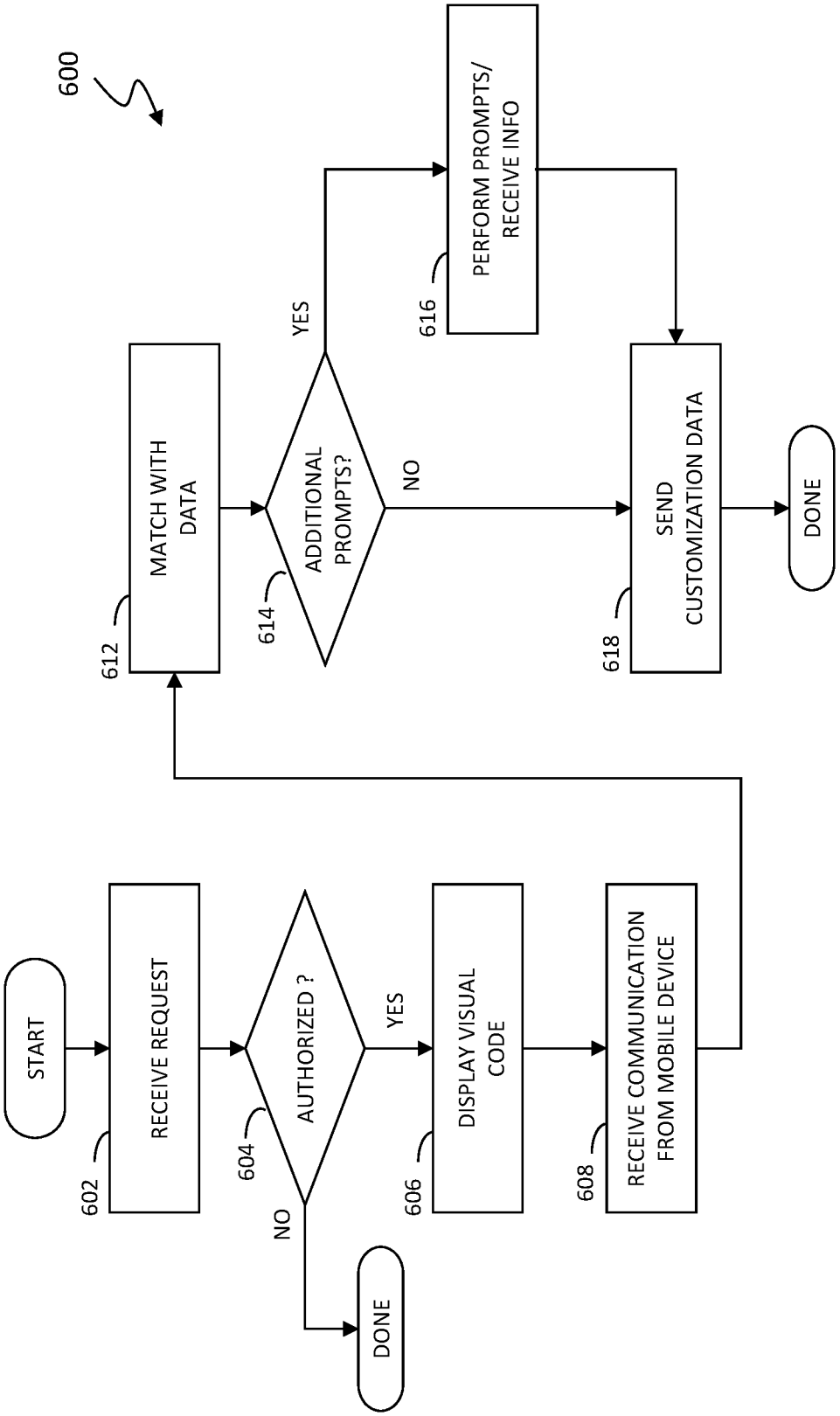

600
START
RECEIVE REQUEST
602
AUTHORIZED ?
604
NO
DONE
YES
DISPLAY VISUAL CODE
606
RECEIVE COMMUNICATION FROM MOBILE DEVICE
608
MATCH WITH DATA
612
ADDITIONAL PROMPTS?
614
YES
PERFORM PROMPTS/ RECEIVE INFO
616
NO
SEND CUSTOMIZATION DATA
618
DONE

FIG. 6

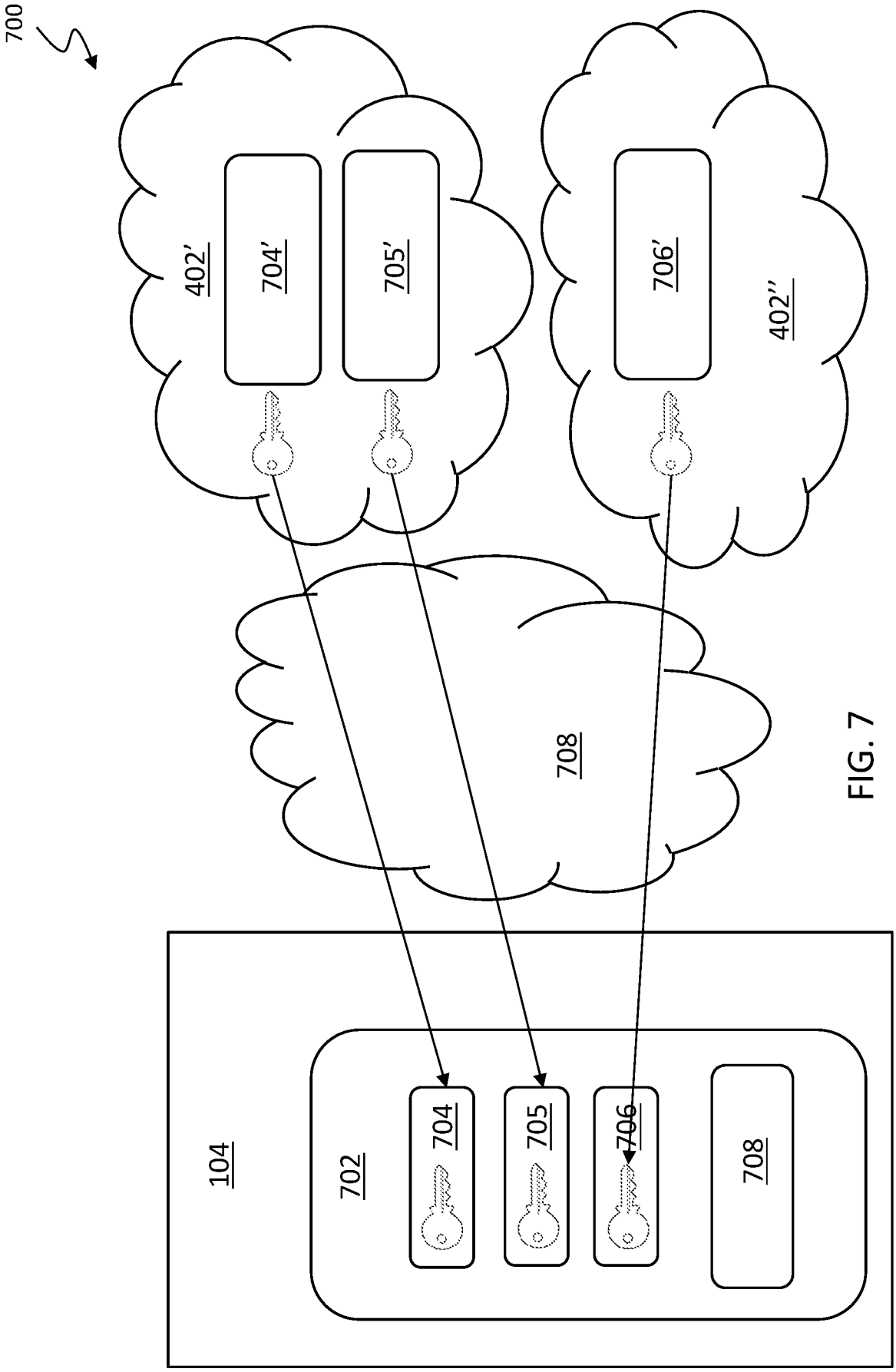


FIG. 7

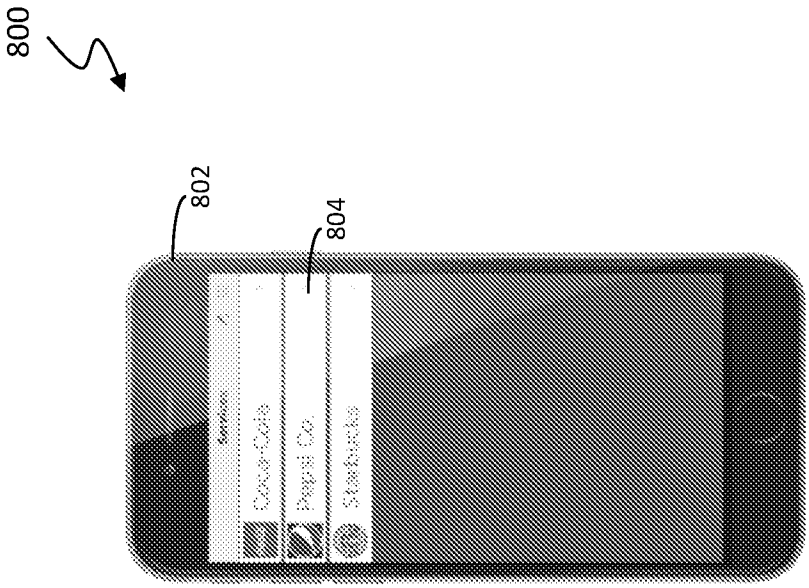


FIG. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2017/001362

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/36 G06F21/42 G06Q20/32 H04L29/06 G06F21/34
H04W12/06 G06Q20/10 G06K7/14
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F G06Q G06K H04L H04W

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2013/050738 A2 (BARCLAYS BANK PLC [GB]) 11 April 2013 (2013-04-11) figure 4 paragraph [0004] - paragraph [0006] paragraph [0043] - paragraph [0060] -----	1-20
A	US 2015/089591 A1 (HARRIS RICHARD H [GB]) 26 March 2015 (2015-03-26) figures 2,3 paragraph [0034] - paragraph [0068] paragraph [0080] - paragraph [0082] -----	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 February 2018	21/02/2018

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2017/001362

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2013050738 A2	11-04-2013	AU 2012320281 A1	22-05-2014
		AU 2017232215 A1	12-10-2017
		CA 2850942 A1	11-04-2013
		EP 2774344 A2	10-09-2014
		GB 2495474 A	17-04-2013
		GB 2495571 A	17-04-2013
		JP 5992528 B2	14-09-2016
		JP 2014531694 A	27-11-2014
		US 2014250512 A1	04-09-2014
		WO 2013050738 A2	11-04-2013
		ZA 201403201 B	29-07-2015
US 2015089591 A1	26-03-2015	AU 2011333497 A1	13-06-2013
		AU 2016225906 A1	29-09-2016
		CA 2818972 A1	31-05-2012
		CL 2013001484 A1	24-01-2014
		CN 103403728 A	20-11-2013
		CN 106127017 A	16-11-2016
		CN 106295303 A	04-01-2017
		CO 6731100 A2	15-08-2013
		EP 2643787 A1	02-10-2013
		GB 2481663 A	04-01-2012
		JP 6141187 B2	07-06-2017
		JP 2014502394 A	30-01-2014
		JP 2017157227 A	07-09-2017
		MX 336021 B	07-01-2016
		RU 2013128748 A	27-12-2014
		US 2015089591 A1	26-03-2015
		WO 2012069845 A1	31-05-2012
		ZA 201303812 B	29-11-2017