



- (51) International Patent Classification:  
*G06Q 20/00* (2012.01)
- (21) International Application Number:  
PCT/EP2017/025367
- (22) International Filing Date:  
21 December 2017 (21.12.2017)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
1621795.2 21 December 2016 (21.12.2016) GB
- (71) Applicant: GURULOGIC MICROSYSTEMS OY  
[FI/FI]; Linnankatu 34, 20100 Turku (FI).
- (72) Inventors: KÄRKKÄINEN, Tuomas; Rautalankatu 2  
B17, 20320 Turku (FI). KALEVO, Ossi; Ketunhätä 1,  
37800 Akaa (FI).
- (74) Agent: NORRIS, Timothy Sweyn; Basck Ltd, 16 Saxon  
Road, Cambridge CB5 8HS, Cambridgeshire (GB).
- (81) Designated States (unless otherwise indicated, for every  
kind of national protection available): AE, AG, AL, AM,  
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,  
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,  
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,  
HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP,  
KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,  
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,  
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,  
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,  
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: SECURE LOG-IN OR TRANSACTION PROCEDURE

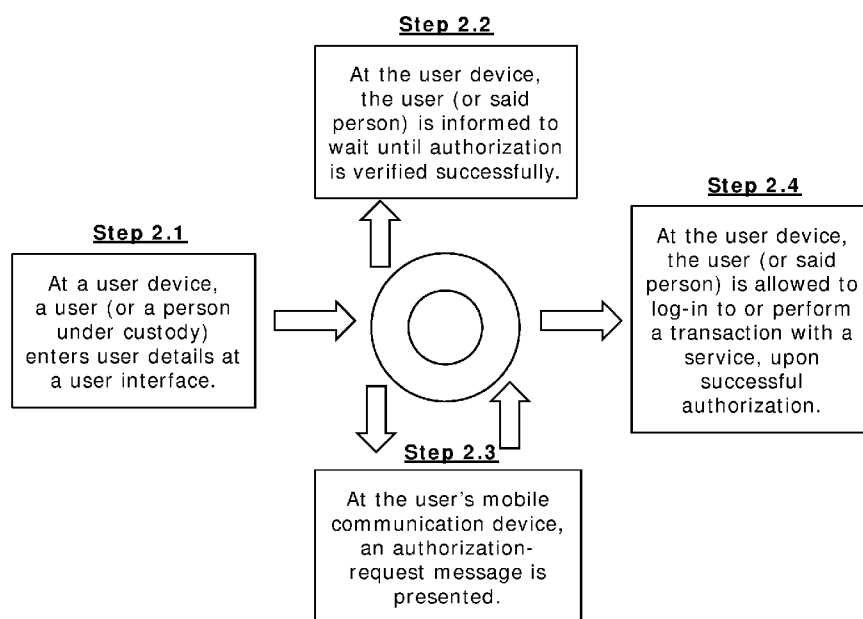


FIG. 2

(57) Abstract: There is provided a method of facilitating a secure log-in procedure or a secure transaction procedure. The method enables a given user or a person under custody of the given user to log-in to or perform a transaction with a service securely. User details entered by the given user or said person at a user interface presented at a user device associated with the given user or said person are received. Subsequently, an authorization-request message is sent to at least one mobile communication device of the given user, using real-time push signalling. A response message indicating whether or not the authorization has been verified successfully is received from the at least one mobile communication device. If the authorization has been verified successfully, the given user or said person is allowed to log-in to or perform a transaction with the service from the user device.



**(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).

**Declarations under Rule 4.17:**

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*
- *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))*

## SECURE LOG-IN OR TRANSACTION PROCEDURE

### TECHNICAL FIELD

The present disclosure relates to systems for facilitating a secure log-in or transaction procedure. Moreover, the present disclosure concerns methods of facilitating a secure log-in or transaction procedure. Furthermore, the present disclosure also relates to computer program products comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute the aforementioned methods.

### BACKGROUND

Various types of secure transactions, for example financial transactions, implemented using chip-enabled debit cards, Internet-based payment services (for example, Paypal<sup>®</sup> and similar), and wirelessly-connected mobile communication devices (for example, smart phones) executing software applications (namely “Apps”), have become widely employed in contemporary commerce. However, there has been a corresponding increase in third-party hostile hacking and malware for acquiring sensitive information, for example passwords, personal identification number (PIN) codes and debit/credit card details, of users. Such acquired sensitive information enables malicious third parties to steal money, or make purchases for their own benefit, at an expense of the users, by the third parties masquerading as the users. For example, sensitive information of a given debit/credit card includes a card number, a username, a term of validity and a verification number of that debit/credit card. A malicious party can easily make financial transactions using this sensitive information of the given debit/credit card on the Internet. A PIN code associated with the given debit/credit card is usually needed only at Point-Of-Sale (POS) terminals, namely when shopping in retail stores. Moreover, strong customer authentication via the PIN code is needed very rarely in online

Internet-based transactions, namely only when a financial transaction is charged from a debit account.

There exist conventional techniques for performing financial transactions in a secure manner. In one conventional technique, a financial institution, for example such as a bank, offers to its customers a software application (namely, an “*App*”) for mobile authorization, wherein the *App* is to be downloaded and installed at the customers’ mobile communication devices. In this conventional technique, a given customer is required to open the *App* on his/her mobile communication device manually, so as to initiate an authorization process using the *App*. This technique is not just user-unfriendly, but also drains a battery of the given customer’s mobile communication device, as the given customer’s mobile communication device has to be kept active for a long duration.

In light of the foregoing, there exists a need for a mobile authorization technique that is user-friendly and that consumes less power.

## **SUMMARY**

The present disclosure seeks to provide an improved system for facilitating a secure log-in or transaction procedure that is highly robust and relatively easy for users to employ, for example, when implementing financial transactions or other types of transactions.

Moreover, the present disclosure seeks to provide an improved method of facilitating a secure log-in or transaction procedure.

A further aim of the present disclosure is to at least partially overcome at least some of the problems of the prior art, as described in the foregoing.

In a first aspect, embodiments of the present disclosure provide a method of facilitating a secure log-in procedure or a secure transaction procedure, to enable a given user or a person under custody of the given user to log-in to or perform a transaction with a service securely, wherein the service is provided by a server arrangement that is coupled via a data communication

network to at least one mobile communication device of the given user, characterized in that the method includes:

- 5 (i) receiving user details entered at a user interface by the given user or the person under custody of the given user, the user interface being presented at a user device associated with the given user or said person for enabling the given user or said person to log-in to or perform the transaction with the service;
- 10 (ii) sending, to the at least one mobile communication device of the given user, an authorization-request message to be presented to the given user for requesting the given user to provide a personal identification code and/or at least one bio-credential of the given user for verifying an authorization, wherein the authorization-request message is sent using real-time push signalling for activating the at least one mobile communication device or an application in the at least one mobile communication device to present the authorization-request message thereat;
- 15 (iii) receiving, from the at least one mobile communication device of the given user, a response message indicating whether or not the authorization has been verified successfully; and
- 20 (iv) allowing the given user or said person to log-in to or perform the transaction with the service from the user device, if the authorization has been verified successfully.

Embodiments of the present disclosure are of advantage in that the  
aforementioned method facilitates a quick, robust and uncomplicated  
25 approach for performing strongly-secured customer authorization.

In a second aspect, embodiments of the present disclosure provide a  
system for facilitating a secure log-in procedure or a secure transaction  
procedure, to enable a given user or a person under custody of the given  
user to log-in to or perform a transaction with a service securely, wherein  
30 the system includes a server arrangement providing the service, the server

arrangement being coupled via a data communication network to at least one mobile communication device of the given user, characterized in that the server arrangement is operable to:

- 5 (i) receive user details entered at a user interface by the given user or the person under custody of the given user, the user interface being presented at a user device associated with the given user or said person for enabling the given user or said person to log-in to or perform the transaction with the service;
- 10 (ii) send, to the at least one mobile communication device of the given user, an authorization-request message to be presented to the given user for requesting the given user to provide a personal identification code and/or at least one bio-credential of the given user for verifying an authorization, wherein the authorization-request message is to be sent using real-time push signalling for  
15 activating the at least one mobile communication device or an application in the at least one mobile communication device to present the authorization-request message thereat;
- (iii) receive, from the at least one mobile communication device of the given user, a response message indicating whether or not the  
20 authorization has been verified successfully; and
- (iv) allow the given user or said person to log-in to or perform the transaction with the service from the user device, if the authorization has been verified successfully.

25 In a third aspect, embodiments of the present disclosure provide a computer program product comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute a method of the aforementioned first aspect.

Additional aspects, advantages, features and objects of the present disclosure would be made apparent from the drawings and the detailed description of the illustrative embodiments construed in conjunction with the appended claims that follow.

- 5 It will be appreciated that features of the present disclosure are susceptible to being combined in various combinations without departing from the scope of the present disclosure as defined by the appended claims.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

The summary above, as well as the following detailed description of  
10 illustrative embodiments, is better understood when read in conjunction with the appended drawings. For the purpose of illustrating the present disclosure, exemplary constructions of the disclosure are shown in the drawings. However, the present disclosure is not limited to specific methods and apparatus disclosed herein. Moreover, those in the art will understand  
15 that the drawings are not to scale. Wherever possible, like elements have been indicated by identical numbers.

Embodiments of the present disclosure will now be described, by way of example only, with reference to the following diagrams wherein:

FIG. 1 is a schematic illustration of a network environment wherein a  
20 system for facilitating a secure log-in procedure or a secure transaction procedure is implemented pursuant to embodiments of the present disclosure;

FIG. 2 is a sequence diagram depicting an example implementation of  
25 a method of facilitating a secure log-in procedure or a secure transaction procedure, in accordance with an embodiment of the present disclosure;

FIGs. 3A and 3B are process flows of example implementations of the  
aforementioned method for enabling a given user (or a person under custody of the given user) to log-in to or perform a

transaction with a service, respectively, pursuant to embodiments of the present disclosure;

5 FIGs. 4A-D are schematic illustrations of example views of user interfaces presented to a given user or a person under custody of the given user at various steps of the example implementation of the aforementioned method; and

10 FIGs. 5A-B is a collection of exemplary views of screenshots of an authorization-request message at the user's mobile communication devices, in accordance with an embodiment of the present disclosure.

In the accompanying drawings, an underlined number is employed to represent an item over which the underlined number is positioned or an item to which the underlined number is adjacent. When a number is non-underlined and accompanied by an associated arrow, the non-underlined  
15 number is used to identify a general item at which the arrow is pointing.

#### **DETAILED DESCRIPTION OF EMBODIMENTS**

The following detailed description illustrates embodiments of the present disclosure and ways in which they can be implemented. Although some modes of carrying out the present disclosure have been disclosed, those  
20 skilled in the art would recognize that other embodiments for carrying out or practising the present disclosure are also possible.

In a first aspect, embodiments of the present disclosure provide a method of facilitating a secure log-in procedure or a secure transaction procedure, to enable a given user or a person under custody of the given user to log-in  
25 to or perform a transaction with a service securely, wherein the service is provided by a server arrangement that is coupled via a data communication network to at least one mobile communication device of the given user, characterized in that the method includes:

30 (i) receiving user details entered at a user interface by the given user or the person under custody of the given user, the user interface



being presented at a user device associated with the given user or said person for enabling the given user or said person to log-in to or perform the transaction with the service;

- 5 (ii) sending, to the at least one mobile communication device of the given user, an authorization-request message to be presented to the given user for requesting the given user to provide a personal identification code and/or at least one bio-credential of the given user for verifying an authorization, wherein the authorization-request message is sent using real-time push signalling for  
10 activating the at least one mobile communication device or an application in the at least one mobile communication device to present the authorization-request message thereat;
- (iii) receiving, from the at least one mobile communication device of the given user, a response message indicating whether or not the  
15 authorization has been verified successfully; and
- (iv) allowing the given user or said person to log-in to or perform the transaction with the service from the user device, if the authorization has been verified successfully.

20 It will be appreciated that the user interface can be presented to the given user or said person via a web browser or a software application running on the user device. It will be further appreciated that the user interface can be presented at any device other than the given user's mobile communication device, for example such as a personal computer or a smartwatch.

25 Optionally, the method includes sending, to the user device, a notification to be presented to the given user or said person for instructing the given user or said person to wait until the authorization via the at least one mobile communication device of the given user has been verified successfully. Optionally, the sending of this notification is performed substantially simultaneously with the sending of the aforementioned authorization-  
30 request message at (ii).

Alternatively, optionally, the method includes configuring the user device to inform the given user or said person to wait, without a need for the notification to be received from the server arrangement. In other words, the user device is optionally configured to inform the given user or said person  
5 on its own, as the user device knows that the authorization is required to be verified.

Yet alternatively, optionally, the given user or said person is not required to be informed at all, as the given user or said person already knows that he/she has to wait until the authorization is verified successfully.

10 Moreover, it will be appreciated that the real-time push signalling is beneficial for sending the authorization-request message at (ii), because such push signalling activates (namely, awakens) the at least one mobile communication device of the given user or the application therein, and displays the authorization-request message to the given user even when a  
15 display screen of the at least one mobile communication device is locked.

According to an embodiment of the present disclosure, in order to be able to awaken the at least one mobile communication device or the application therein via such push signalling, a push notification service provided by an ecosystem of the at least one mobile communication device is required to  
20 be enabled on the at least one mobile communication device. Examples of such push notification services include, but are not limited to, Apple® Push Notification service (APNs), Google® Cloud Messaging (GCM), and Windows® Notification Service (WNS).

Optionally, in this regard, such push signalling activates (namely, awakens)  
25 a trusted software application (namely, the aforesaid application) on the at least one mobile communication device, wherein the trusted software application is previously provided to the at least one mobile communication device by the server arrangement. This allows the given user to provide the personal identification code and/or the at least one bio-credential of the  
30 given user without wasting any time (namely promptly), and thus, without draining a battery of the at least one mobile communication device

unnecessarily, because the aforementioned method requires that the at least one mobile communication device of the given user is active only for the time needed for performing the authorization. Notably, contemporary known techniques are based on pull technology, and require an end user to open a software application (namely, *App*) manually on his/her mobile communication device, prior to initiating an authorization process. Such contemporary known techniques are not only inconvenient to the end user, but also drain a battery of the end user's mobile communication device for a longer time, as compared to the method pursuant to embodiments of the present disclosure.

According to another embodiment of the present disclosure, the aforementioned push signalling is implemented by way of a trusted software application that is executing in the background at the at least one mobile communication device, wherein the trusted software application is operable to receive a push signal from the server arrangement to awaken the at least one mobile communication device, and to present the authorization-request message at the at least one mobile communication device in real time or near real time.

Regardless of any specific embodiment of the present disclosure, a service provider can generate at the at least one mobile communication device an event, for example, such as an image or a link, acting as a request for the user to confirm.

Moreover, according to an embodiment of the present disclosure, the at least one mobile communication device of the given user includes a plurality of mobile communication devices of the given user that are registered with the server arrangement. Optionally, in such a case, the authorization-request message is sent to each of the plurality of mobile communication devices of the given user at (ii).

Optionally, in such a case, when the response message is received from any one of the plurality of mobile communication devices at (iii), the method includes sending, to rest of the plurality of mobile communication devices,

an instruction to ignore the authorization-request message that was previously sent at (ii).

Moreover, optionally, the method includes keeping a track of which mobile communication device has been used to perform the authorization.

5 Optionally, in this regard, the method includes maintaining a log of a given mobile communication device that was used to perform the authorization and its associated timestamp.

Maintaining such a log over a period of time is particularly beneficial for investigative purposes, for example, in a case when the given user did not  
10 perform the authorization himself or herself. Optionally, in this regard, the method includes blocking a given mobile communication device of the given user from which an unauthorized party has made an attempt to perform the authorization, so as to avoid any further abuse.

Optionally, in order to register the at least one mobile communication  
15 device with the server arrangement, the method includes providing a trusted software application (for example, an “App”) to the at least one mobile communication device, wherein the trusted software application is then installed at the at least one mobile communication device. More optionally, the trusted software application is provided to the at least one  
20 mobile communication device in an encrypted form.

Optionally, in the method, the trusted software application is operable to compare the personal identification code and/or the at least one bio-credential provided by the given user with a previously-registered personal identification code and/or at least one bio-credential of the given user,  
25 namely a personal identification code and/or at least one bio-credential of the given user previously registered with the trusted software application. Alternatively, optionally, the comparison is performed by the ecosystem of the at least one mobile communication device.

Optionally, the trusted software application is then operable to determine whether or not the authorization has been verified successfully, based upon the comparison.

Optionally, in the method, the trusted software application is operable to  
5 employ at least one key that is stored in a key store of the at least one mobile communication device to encrypt the response message.

Additionally or alternatively, optionally, the trusted software application is operable to employ a certificate that is stored in the key store of the at least one mobile communication device to sign digitally the response message.

10 In other words, the response message may be any one of:

- (i) encrypted using the at least one key,
- (ii) digitally signed using the certificate, or
- (iii) both encrypted (using the at least one key) and digitally signed (using the certificate).

15 Optionally, by providing the personal identification code and/or the at least one bio-credential, the given user authorizes the trusted software application to sign digitally the content of the response message using his/her own private key (for example, for a Public Key Infrastructure (PKI) equivalent usage). This enables the server arrangement to verify the given  
20 user as its registered client, using a public key registered for the given user.

Optionally, the content of the response message is the same as the content of the authorization-request message. Optionally, in such a case, when the response message is digitally signed using a private key and/or a certificate of the key store, the server arrangement is operable to verify that the  
25 content of the response message that is delivered back is unchanged from the content of the authorization-request message that was previously sent at (ii).

It will be appreciated that when the response message is received in encrypted form, the method includes decrypting the response message.

Moreover, optionally, the response message is received from the at least one mobile communication device, via secured transportation. Such secured transportation can be implemented, for example, via HyperText Transport Protocol Secure (HTTPS) protocol or Secure Sockets Layer (SSL).

Optionally, the method includes providing the at least one mobile communication device with the key store including keys and/or certificates to be used for encryption and/or decryption purposes and/or signing purposes, respectively. The key store may, for example, be provided by the server arrangement or a trusted third party.

Optionally, in the method, the usage of the key store is protected in operation, such that the contents of the key store are accessible to the trusted software application only. Optionally, in the method, the usage of the key store is protected in operation by a kernel layer of the at least one mobile communication device. Optionally, the kernel layer of the at least one mobile communication device is implemented as a mixture of hardware and software, and is proprietary to the at least one mobile communication device, for example is proprietary to a manufacturer of the at least one mobile communication device. However, it will be appreciated that a protected key store is optionally provided by using other security methods, for example by employing heavy data encryption, or by employing a combination of heavy data encryption following by data obfuscation for securing data, and an inverse of such heavy encryption when recovering data. Obfuscation is optionally achieved by inverting and/or swapping specific bits of data bytes.

Optionally, the aforementioned trusted software application is operable to interface with other software applications executing in other software layers hosted, in operation, in the at least one mobile communication device. In other words, in operation, various data exchanges occur between the trusted software application executing in the kernel layer and the other

software applications executing in the software layers. Optionally, in such a case, the aforementioned trusted software application is protected by security provisions of the kernel layer that are typically more secure than the software layers.

5   Optionally, in this regard, the trusted software application is executed in a secure area of processing hardware of the at least one mobile communication device. More optionally, the secure area of the processing hardware is implemented by way of Trusted Execution Environment (TEE; see reference [1]).

10   Moreover, optionally, the method includes aborting the secure log-in procedure or the secure transaction procedure, if no response message is received from the at least one mobile communication device of the given user within a predefined time period. In some examples, the predefined time period optionally is in a range of a few seconds to tens of seconds. In  
15   other examples, the predefined time period is optionally longer, and is optionally in a range of tens of seconds to a few minutes. In such cases, an additional feature is optionally provided in the authorization-request message that enables the given user to decline the authorization request, for example, when the given user no longer wants to make the financial  
20   transaction.

It will be appreciated that when the predefined time period is shorter, there is no need for providing the aforementioned feature, as the at least one mobile communication device is useable again within a short time period, without a need to decline the authorization request. On the other hand,  
25   when the predefined time period is too short, there potentially arises a situation where the given user is not able to respond to the authorization request within the time period, even when the given user is interested in logging-in to or performing the transaction with the service. However, for security purposes, it is desirable to define the predefined time period to be  
30   as short as practically possible.

Optionally, in the method, the personal identification code is a Personal Identification Number (PIN) code. It will be appreciated that the personal identification code can alternatively be a code that includes alphanumeric characters and/or special characters that can be entered using a keypad of  
5 the at least one mobile communication device.

Optionally, the at least one bio-credential of the given user includes at least one of: a fingerprint of the given user, facial features of the given user, iris recognition of the given user, DNA genetic information of the given user. As an example, a fingerprint or a facial image of the given user can be  
10 captured via an image sensor of the at least one mobile communication device of the given user. It will be appreciated that the given user's bio-credential may alternatively correspond to any other type of biometrical verification feasible in future, for example by employing a bio-sensor to provide a DNA analysis of the user's sweat or sputum. Optionally,  
15 alternatively, the bio-credential can include for example a walking manner of the given user, a writing manner of the given user or a heartbeat pattern of the given user, depending on the feasibility in the service area in question. It will be appreciated that it does not matter what kind of verification method is used for embodiments of the present disclosure, as it  
20 is typically the at least one mobile communication device that defines such an operation.

Examples of the user device and the at least one mobile communication device include, but are not limited to, mobile phones, smart telephones, smartwatches, Mobile Internet Devices (MIDs), tablet computers, Ultra-  
25 Mobile Personal Computers (UMPCs), phablet computers, Personal Digital Assistants (PDAs), web pads, Personal Computers (PCs), handheld PCs, laptop computers, desktop computers, and large-sized touch screens with embedded PCs. Some specific examples of such devices include, but are not limited to, iPhone®, iPad®, Android® phone, Android® web pad, Windows®  
30 phone, and Windows® web pad.

Moreover, the data communication network can be a collection of individual networks, interconnected with each other and functioning as a single large



network. Such individual networks may be wired, wireless, or a combination thereof. Examples of such individual networks include, but are not limited to, Local Area Networks (LANs), Wide Area Networks (WANs), Metropolitan Area Networks (MANs), Wireless LANs (WLANs), Wireless WANs (WWANs),  
5 Wireless MANs (WMANs), the Internet, second generation (2G) telecommunication networks, third generation (3G) telecommunication networks, fourth generation (4G) telecommunication networks, fifth generation (5G) telecommunication networks, community networks, satellite networks, vehicular networks, sensor networks, and Worldwide  
10 Interoperability for Microwave Access (WiMAX) networks.

Furthermore, it will be appreciated that the aforementioned method is suitable to be implemented for various purposes, for example, such as making financial transactions, logging-in to a secure service, casting a vote and other services that require a strong customer authorization.

15 Optionally, in the method, the transaction pertains to at least one of: a financial payment, digital signing. As an example, when the transaction pertains to a financial payment, the service is implemented as a payment service using which the given user or said person makes the financial payment. As another example, when the transaction pertains to digital  
20 signing, the service is implemented as a digital signature service using which the given user or said person signs, for example, a given electronic document digitally.

Furthermore, it will be appreciated that said person may be a child, an elder person, or any other person who is under custody of the given user. As an  
25 example, the aforementioned method can be implemented for parental guidance, for example, when a parent (namely, the given user) wishes to administer a payment made by his/her minor-aged child or to administer his/her child's attempt to access an entertainment service (for example, an online game site or similar). As another example, the aforementioned  
30 method can be implemented for monitoring elderly people; notably, it is often desired to control their usage of funds, when they become incapable of understanding the impact of their actions and the value of money.

It will be appreciated that the aforementioned method may be implemented not only when said person wants to log-in to a web service (for example, such as an online gaming service, an online video-streaming service and the like), but also when said person wants to access certain sections of the web service. In other words, upon logging-in to the web service, some sections of the web service may be accessible to said person (for example, a minor-aged child), while other sections of the web service may not be freely accessible to said person. In such a case, said person would require similar authorization verifications when accessing these other sections of the web service.

Optionally, in the method, the server arrangement is implemented to provide a background service that is configured to perform the aforementioned steps (i) to (iv), wherein the background service is separate from the aforementioned service. In some implementations, the background service is provided by a background service provider that is different from the service provider providing the service. In other implementations, the background service is provided by the service provider itself.

For illustration purposes only, there will now be considered an example implementation of the aforementioned method pursuant to embodiments of the present disclosure, wherein a payment service provided by a service provider is linked to a background service provided by a background service provider. One such example implementation has been illustrated in conjunction with FIGs. 3A and 3B. In the illustrated example, the method is performed in multiple steps, for example, as follows:

Step 1:

In a user interface, for example a web browser, of a user device, a log-in page (namely, for logging-in to the payment service and/or to make a financial transaction using the payment service) is presented to a given user or a person under custody of the given user. On the log-in page, the given user or said person provides his/her user details (for example, such as his/her username, e-mail address, phone number, account number, social

security number and similar), if his/her user details are not already cached in the web browser.

The user device sends, to the service provider, the user details along with a request to initiate a secure session to access the payment service. The  
5 background service provider listens to the session request incoming at the service provider.

Step 2 (Optional):

The service provider sends, to the user device, a notification to wait until authorization via a user's registered mobile communication device has been  
10 verified successfully. Alternatively, optionally, the user device informs the given user or said person to wait, without a need for the notification to be received from the service provider. In other words, the user device optionally informs the given user or said person on its own, as the user device knows that the authorization is required to be verified.

15 Step 3:

The background service provider sends, to the user's registered mobile communication device (or devices), an authorization-request message using real-time push signalling. As a result, the user's registered mobile communication device or an application therein awakens, and presents the  
20 authorization-request message to the given user.

Optionally, the steps 2 and 3 are performed substantially simultaneously.

Step 4:

The given user provides his/her personal identification code and/or his/her bio-credential at the user's registered mobile communication device. A  
25 trusted software application of the user's registered mobile communication device then sends, to the background service provider, a response message indicating whether or not the authorization has been verified successfully.

Step 5:

The background service provider routes the response message to the service provider.

Step 6:

5 Upon successful verification of the authorization, the log-in page at the user device redirects to a protected site, thereby allowing the given user or said person to access the payment service provided by the service provider. Otherwise, the log-in page is redirected to a page showing log-in failure or timeout.

10 In a second aspect, embodiments of the present disclosure provide a system for facilitating a secure log-in procedure or a secure transaction procedure, to enable a given user or a person under custody of the given user to log-in to or perform a transaction with a service securely, wherein the system includes a server arrangement providing the service, the server arrangement being coupled via a data communication network to at least  
15 one mobile communication device of the given user, characterized in that the server arrangement is operable to:

- (i) receive user details entered at a user interface by the given user or the person under custody of the given user, the user interface being presented at a user device associated with the given user or  
20 said person for enabling the given user or said person to log-in to or perform the transaction with the service;
- (ii) send, to the at least one mobile communication device of the given user, an authorization-request message to be presented to the given user for requesting the given user to provide a personal  
25 identification code and/or at least one bio-credential of the given user for verifying an authorization, wherein the authorization-request message is to be sent using real-time push signalling for activating the at least one mobile communication device or an application in the at least one mobile communication device to  
30 present the authorization-request message thereat;

- (iii) receive, from the at least one mobile communication device of the given user, a response message indicating whether or not the authorization has been verified successfully; and
- (iv) allow the given user or said person to log-in to or perform the transaction with the service from the user device, if the authorization has been verified successfully.

Optionally, the server arrangement is operable to send, to the user device, a notification to be presented to the given user or said person for instructing the given user or said person to wait until the authorization via the at least one mobile communication device of the given user has been verified successfully.

According to an embodiment of the present disclosure, in order to be able to awaken the at least one mobile communication device or the application therein via such push signalling, a push notification service provided by an ecosystem of the at least one mobile communication device is required to be enabled on the at least one mobile communication device. Examples of such push notification services include, but are not limited to, Apple® Push Notification service (APNs), Google® Cloud Messaging (GCM), and Windows® Notification Service (WNS).

According to another embodiment of the present disclosure, the aforementioned push signalling is implemented by way of a trusted software application (namely, the aforementioned application) that is executing in the background at the at least one mobile communication device, wherein the trusted software application is operable to receive a push signal from the server arrangement to awaken the at least one mobile communication device, and to present the authorization-request message at the at least one mobile communication device in real time or near real time.

Moreover, according to an embodiment of the present disclosure, the at least one mobile communication device of the given user includes a plurality of mobile communication devices of the given user that are registered with

the server arrangement. Optionally, in such a case, the server arrangement is operable to send the authorization-request message to each of the plurality of mobile communication devices of the given user at (ii).

Optionally, in such a case, when the response message is received from any one of the plurality of mobile communication devices at (iii), the server arrangement is operable to send, to rest of the plurality of mobile communication devices, an instruction to ignore the authorization-request message that was previously sent at (ii).

Moreover, optionally, the server arrangement is operable to keep a track of which mobile communication device has been used to perform the authorization. Optionally, in this regard, the server arrangement is operable to maintain a log of a given mobile communication device that was used to perform the authorization and its associated timestamp.

Optionally, the system includes a database arrangement coupled in communication with the server arrangement. Optionally, in such a case, the log is to be maintained at the database arrangement.

Optionally, the server arrangement and the database arrangement are implemented by way of cloud computing services.

Optionally, in order to register the at least one mobile communication device with the server arrangement, the server arrangement is operable to provide a trusted software application (for example, an "App") to the at least one mobile communication device, wherein the trusted software application is then installed at the at least one mobile communication device. More optionally, the server arrangement is operable to provide the trusted software application to the at least one mobile communication device in encrypted form.

Optionally, the trusted software application is operable to compare the personal identification code and/or the at least one bio-credential provided by the given user with a previously-registered personal identification code and/or at least one bio-credential of the given user. Alternatively,

optionally, the comparison is performed by the ecosystem of the at least one mobile communication device.

Optionally, the trusted software application is then operable to determine whether or not the authorization has been verified successfully, based upon  
5 the comparison.

Optionally, the trusted software application is operable to employ at least one key that is stored in a key store of the at least one mobile communication device to encrypt the response message.

Additionally or alternatively, optionally, the trusted software application is  
10 operable to employ a certificate that is stored in the key store of the at least one mobile communication device to digitally sign the response message.

Optionally, in this regard, the server arrangement is operable to provide the at least one mobile communication device with the key store including keys and/or certificates to be used for encryption and/or decryption purposes  
15 and/or signing purposes, respectively. Alternatively, optionally, the key store is provided by a trusted third party.

Optionally, the usage of the key store is protected in operation, such that the contents of the key store are accessible to the trusted software application only. Optionally, the usage of the key store is protected in  
20 operation by a kernel layer of the at least one mobile communication device. Optionally, in this regard, the trusted software application is executed in a secure area of processing hardware of the at least one mobile communication device. More optionally, the secure area of the processing hardware is implemented by way of TEE (see reference [1]).

25 Moreover, optionally, the server arrangement is operable to abort the secure log-in procedure, if no response message is received from the at least one mobile communication device of the given user within a predefined time period.

Optionally, the at least one bio-credential of the given user includes at least one of: a fingerprint of the given user, facial features of the given user, iris recognition of the given user, DNA genetic information of the given user.

Furthermore, optionally, the server arrangement is implemented to provide  
5 a background service that is configured to perform the aforesaid (i) to (iv),  
wherein the background service is separate from the aforementioned  
service. In some implementations, the background service is provided by a  
background service provider that is different from a service provider  
providing the service. In other implementations, the background service is  
10 provided by the service provider itself.

Optionally, the transaction pertains to at least one of: a financial payment,  
digital signing. As an example, the service could be a payment service using  
which the given user or said person makes the financial payment. As  
another example, the service could be a digital signature service using  
15 which the given user or said person signs, for example, a given electronic  
document digitally.

In a third aspect, embodiments of the present disclosure provide a  
computer program product comprising a non-transitory computer-readable  
storage medium having computer-readable instructions stored thereon, the  
20 computer-readable instructions being executable by a computerized device  
comprising processing hardware to execute a method of the aforementioned  
first aspect.

Optionally, the computer-readable instructions are downloadable from a  
software application store, for example, from an "App store" to the  
25 computerized device.

Next, embodiments of the present disclosure will be described with  
reference to figures.

FIG. 1 is a schematic illustration of a network environment **100** wherein a  
system for facilitating a secure log-in procedure or a secure transaction  
30 procedure is implemented pursuant to embodiments of the present



disclosure. The system includes a server arrangement **102** providing a service and a database arrangement **104** associated with the server arrangement **102**.

In the network environment **100**, the server arrangement **102** is coupled in  
5 communication with a user device **106** of a given user or a person under custody of the given user and with at least one mobile communication device of the given user, depicted as a mobile communication device **108** in FIG. 1, via a data communication network **110**.

The server arrangement **102** is operable to perform operations, for  
10 example, as described with respect to the aforementioned second aspect. These operations include:

- (i) receiving user details entered by the given user or said person at a user interface presented at the user device **106** for enabling the given user or said person to log-in to or perform a transaction with the service;  
15
- (ii) sending, to the mobile communication device **108**, an authorization-request message to be presented to the given user for requesting the given user to provide a personal identification code and/or at least one bio-credential of the given user for verifying an authorization, wherein the authorization-request message is sent using real-time push signalling for activating the mobile communication device **108** or an application in the mobile communication device **108** to present the authorization-request message thereat;  
20
- (iii) receiving, from the mobile communication device **108**, a response message indicating whether or not the authorization has been verified successfully; and  
25
- (iv) allowing the given user or said person to log-in to or perform the transaction with the service from the user device **106**, if the authorization has been verified successfully.  
30

FIG. 1 is merely an example, which should not unduly limit the scope of the claims herein. It is to be understood that the specific designation for the network environment **100** is provided as an example and is not to be construed as limiting the network environment **100** to specific numbers, types, or arrangements of server arrangements, database arrangements, user devices, mobile communication devices, and data communication networks. A person skilled in the art will recognize many variations, alternatives, and modifications of embodiments of the present disclosure.

Referring next to FIG. 2, there is provided a sequence diagram depicting an example implementation of a method of facilitating a secure log-in procedure or a secure transaction procedure, in accordance with an embodiment of the present disclosure. The method enables a given user or a person under custody of the given user to log-in to or perform a transaction with a service securely.

At a step **2.1**, the given user or said person provides his/her user details (for example, such as his/her username, e-mail address, phone number or similar) on a user interface presented at a user device of the given user or said person. The user details are received at a server arrangement providing the aforesaid service.

At a step **2.2**, the server arrangement optionally sends a notification to the user device to inform the given user or said person to wait until authorization via a user's registered mobile communication device has been verified successfully. Alternatively, optionally, the user device informs the given user or said person to wait, without a need for the notification to be received from the server arrangement. In other words, the user device optionally informs the given user or said person on its own, as the user device knows that the authorization is required to be verified. Yet alternatively, optionally, the given user or said person is not required to be informed at all, as the given user or said person already knows that he/she has to wait until the authorization is verified successfully.

At a step **2.3**, the server arrangement sends an authorization-request message to the user's registered mobile communication device (or devices) using real-time push signalling.

Optionally, the steps **2.2** and **2.3** are performed substantially  
5 simultaneously.

At this step, the given user provides his/her personal identification code and/or at least one bio-credential at the user's registered mobile communication device.

Accordingly, a response message is sent from the user's registered mobile  
10 communication device to the server arrangement.

At a step **2.4**, upon successful verification of the authorization, the given user or said person is allowed to log-in to or perform the transaction with the service from the user device.

The steps **2.1** to **2.4** are only illustrative and other alternatives can also be  
15 provided where one or more steps are added without departing from the scope of the claims herein.

FIG. 3A is a process flow of an example implementation of the  
aforementioned method for enabling a given user (or a person under  
custody of the given user) to log-in to a service, in accordance with an  
20 embodiment of the present disclosure.

In the example implementation, the service is a web service (for example, such as an online gaming service, an online video-streaming service, online payment service and the like) provided by a service provider. The service is linked to a background service provided by a background service provider.  
25 In the illustrated example, the method is performed in multiple steps as follows:

Step 1:

In a user interface, for example a web browser, of a user device, a log-in page (namely, for logging-in to the service) is presented to the given user or said person. On the log-in page, the given user or said person provides his/her user details (for example, such as his/her username, user ID, e-mail address, phone number, account number, social security number and similar), if his/her user details are not already cached in the web browser.

The user device sends, to the service provider, the user details along with a request to initiate a secure session to access the service. The service provider sends the user details to the background service provider, which then listens to the session request incoming at the service provider.

Step 2:

The background service provider sends, to the user's registered mobile communication device (or devices), an authorization-request message using real-time push signalling. As a result, the user's registered mobile communication device or an application therein awakens, and presents the authorization-request message to the given user.

Step 3:

If the request is justified, the given user verifies the authorization by providing his/her personal identification code and/or his/her bio-credential at the user's registered mobile communication device. A trusted software application of the user's registered mobile communication device then sends, to the background service provider, a response message indicating whether or not the authorization has been verified successfully.

Step 4:

The background service provider routes the response message to the service provider.

Step 5:

Upon successful verification of the authorization, the log-in page at the user device redirects to a protected site, thereby allowing the given user or said person to access the service provided by the service provider. Otherwise, the log-in page is redirected to a page showing log-in failure or timeout.

5 It will be appreciated that upon successful log-in to the web service (for example, such as an online gaming service, an online video-streaming service and the like), some sections of the web service may be accessible to said person (for example, a child), while other sections of the web service may not be freely accessible to said person. In such a case, said person  
10 might require further authorization verifications when accessing certain sections of the web service. Such authorization verifications may be performed in a manner that is similar to the aforementioned process flow elucidated in conjunction with FIG. 3A.

FIG. 3B is a process flow of an example implementation of the  
15 aforementioned method for enabling the given user (or said person) to perform a transaction with the service, in accordance with an embodiment of the present disclosure.

In the example implementation, the service is implemented as an online payment service using which the given user or said person perform a  
20 financial payment transaction. In the illustrated example, the method is performed in multiple steps as follows:

Step 1:

In the user interface of the user device, a transaction page (namely, for performing the transaction with the service) is presented to the given user  
25 or said person. On the transaction page, the given user or said person provides his/her user details, if his/her user details are not already cached.

The user device sends, to the service provider, the user details along with a request to initiate a secure session to perform the transaction. The service provider sends the user details to the background service provider, which  
30 then listens to the session request incoming at the service provider.

Step 2:

The background service provider sends, to the user's registered mobile communication device (or devices), an authorization-request message using real-time push signalling. As a result, the user's registered mobile communication device or an application therein awakens, and presents the authorization-request message to the given user.

Step 3:

If the request is justified, the given user verifies the authorization by providing his/her personal identification code and/or his/her bio-credential at the user's registered mobile communication device. A trusted software application of the user's registered mobile communication device then sends, to the background service provider, a response message indicating whether or not the authorization has been verified successfully.

Step 4:

The background service provider routes the response message to the service provider.

Step 5:

Upon successful verification of the authorization, the given user or said person is allowed to perform the transaction with the service. Otherwise, the transaction page is redirected to a page showing transaction failure or timeout.

FIGs. 3A and 3B are merely examples, which should not unduly limit the scope of the claims herein. A person skilled in the art will recognize many variations, alternatives, and modifications of embodiments of the present disclosure.

FIGs. 4A, 4B, 4C and 4D are schematic illustrations of example views of user interfaces presented to the given user or the person under custody of the given user at the steps 2.1, 2.2, 2.3 and 2.4 of FIG. 2, respectively.

The exemplary service in the mentioned figures is a communication and conferencing service provided by Gurulogic Microsystem Oy's proprietary product "Starwindow®").

FIG. 4A is a schematic illustration of a first example view of a first user interface that is presented at the user device of the given user or said person, wherein the given user or said person enters his username bob@example.com at a Starwindow® log-in page presented in the first example view.

FIG. 4B is a schematic illustration of a second example view of the first user interface that is presented at the user device of the given user or said person, wherein the given user or said person is informed to wait until biometric verification is performed.

FIG. 4C is a schematic illustration of an example view of a second user interface that is presented at the mobile communication device of the given user, wherein the authorization-request message is presented to the given user. In this example view, the given user is requested to perform a biometric verification by way of presenting a fingerprint of the given user to an image sensor of the mobile communication device, within a predefined time period of three minutes.

Optionally, a contact field, denoted by "X" in the example view, is provided in case the given user changes his/her mind and no longer wants to log-in to the service.

FIG. 4D is a schematic illustration of a third example view of the first user interface that is presented at the user device of the given user or said person, wherein the given user or said person is allowed to log-in to the Starwindow® service, upon successful verification of the authorization, and a confirmation screen is presented to the given user or said person.

FIGs. 4A-D are merely examples, which should not unduly limit the scope of the claims herein. A person skilled in the art will recognize many variations, alternatives, and modifications of embodiments of the present disclosure.

Referring next to FIGs. 5A and 5B, there are shown examples of authorization-request messages that are presented to the given user via user interfaces provided, in operation, on different mobile communication devices of the given user, for example such as a smart phone, a smart watch, smart electronically-enabled clothing or similar, when logging-in to or performing a transaction with a service pursuant to embodiments of the present disclosure. In respect of a smart phone depicted in FIG. 5A for purposes of an authorization request of a log-in procedure, an e-mail address detail is provided, together with an amount of time remaining for the given user to respond by sending a confirmation via the user interface. Optionally, beneficially, in the middle at the bottom, there is an option for biometric verification, for example via fingerprint credentials. Moreover, in respect of a smart watch depicted in FIG. 5B for purposes of an authorization-request of a financial transaction, an e-mail address detail is provided, together with a sum of money to be paid, and buttons for enabling the given user either to confirm via the user interface a payment of the sum of money or to decline such payment.

FIGs. 5A and 5B are merely examples, which should not unduly limit the scope of the claims herein. A person skilled in the art will recognize many variations, alternatives, and modifications of embodiments of the present disclosure.

Modifications to embodiments of the present disclosure described in the foregoing are possible without departing from the scope of the present disclosure as defined by the accompanying claims. Expressions such as “including”, “comprising”, “incorporating”, “consisting of”, “have”, “is” used to describe and claim the present invention are intended to be construed in a non-exclusive manner, namely allowing for items, components or elements not explicitly described also to be present. Reference to the singular is also to be construed to relate to the plural; as an example, “*at least one of*” indicates “*one of*” in an example, and “*a plurality of*” in another example; moreover, “*two of*”, and similarly “one or more” are to be construed in a likewise manner.



The phrases “in an embodiment”, “according to an embodiment” and the like generally mean the particular feature, structure, or characteristic following the phrase is included in at least one embodiment of the present disclosure, and may be included in more than one embodiment of the present disclosure. Importantly, such phrases do not necessarily refer to the same embodiment.

## REFERENCES

- [1] Trusted execution environment - Wikipedia, the free encyclopedia (accessed December 12, 2016); URL: [https://en.wikipedia.org/wiki/Trusted\\_execution\\_environment](https://en.wikipedia.org/wiki/Trusted_execution_environment)

**CLAIMS**

We claim:

1. A method of facilitating a secure log-in procedure or a secure  
5 transaction procedure, to enable a given user or a person under custody of  
the given user to log-in to or perform a transaction with a service securely,  
wherein the service is provided by a server arrangement that is coupled via  
a data communication network to at least one mobile communication device  
of the given user, characterized in that the method includes:
- 10 (i) receiving user details entered at a user interface by the given user  
or the person under custody of the given user, the user interface  
being presented at a user device associated with the given user or  
said person for enabling the given user or said person to log-in to  
or perform the transaction with the service;
- 15 (ii) sending, to the at least one mobile communication device of the  
given user, an authorization-request message to be presented to  
the given user for requesting the given user to provide a personal  
identification code and/or at least one bio-credential of the given  
20 user for verifying an authorization, wherein the authorization-  
request message is sent using real-time push signalling for  
activating the at least one mobile communication device or an  
application in the at least one mobile communication device to  
present the authorization-request message thereat;
- (iii) receiving, from the at least one mobile communication device of  
25 the given user, a response message indicating whether or not the  
authorization has been verified successfully; and
- (iv) allowing the given user or said person to log-in to or perform the  
transaction with the service from the user device, if the  
authorization has been verified successfully.

2. A method of claim 1, characterized in that the transaction pertains to at least one of: a financial payment, digital signing.

3. A method of claim 1 or 2, characterized in that the method includes sending, to the user device, a notification to be presented to the given user or said person for instructing the given user or said person to wait until the authorization via the at least one mobile communication device of the given user has been verified successfully.

4. A method of claim 1, 2 or 3, characterized in that the at least one mobile communication device of the given user includes a plurality of mobile communication devices of the given user that are registered with the server arrangement, wherein when the response message is received from any one of the plurality of mobile communication devices at (iii), the method includes sending, to rest of the plurality of mobile communication devices, an instruction to ignore the authorization-request message sent at (ii).

5. A method of claim 1, 2, 3 or 4, characterized in that the method includes maintaining a log of a given mobile communication device that was used to perform the authorization and its associated timestamp.

6. A method of any one of claims 1 to 5, characterized in that the at least one bio-credential of the given user includes at least one of: a fingerprint of the given user, facial features of the given user, iris recognition of the given user, DNA genetic information of the given user.

7. A method of any one of claims 1 to 6, characterized in that the response message is received in an encrypted form.

8. A system for facilitating a secure log-in procedure or a secure transaction procedure, to enable a given user or a person under custody of the given user to log-in to or perform a transaction with a service securely, wherein the system includes a server arrangement providing the service, the server arrangement being coupled via a data communication network to at least one mobile communication device of the given user, characterized in that the server arrangement is operable to:

- 5 (i) receive user details entered at a user interface by the given user or the person under custody of the given user, the user interface being presented at a user device associated with the given user or said person for enabling the given user or said person to log-in to or perform the transaction with the service;
- 10 (ii) send, to the at least one mobile communication device of the given user, an authorization-request message to be presented to the given user for requesting the given user to provide a personal identification code and/or at least one bio-credential of the given user for verifying an authorization, wherein the authorization-request message is to be sent using real-time push signalling for activating the at least one mobile communication device or an application in the at least one mobile communication device to present the authorization-request message thereat;
- 15 (iii) receive, from the at least one mobile communication device of the given user, a response message indicating whether or not the authorization has been verified successfully; and
- 20 (iv) allow the given user or said person to log-in to or perform the transaction with the service from the user device, if the authorization has been verified successfully.

9. A system of claim 8, characterized in that the transaction pertains to at least one of: a financial payment, digital signing.

25 10. A system of claim 8 or 9, characterized in that the server arrangement is operable to send, to the user device, a notification to be presented to the given user or said person for instructing the given user or said person to wait until the authorization via the at least one mobile communication device of the given user has been verified successfully.

30 11. A system of claim 8, 9 or 10, characterized in that the at least one mobile communication device of the given user includes a plurality of mobile communication devices of the given user that are registered with the server

arrangement, wherein when the response message is received from any one of the plurality of mobile communication devices at (iii), the server arrangement is operable to send, to rest of the plurality of mobile communication devices, an instruction to ignore the authorization-request  
5 message sent at (ii).

12. A system of any one of claims 8 to 11, characterized in that the server arrangement is operable to maintain a log of a given mobile communication device that was used to perform the authorization and its associated timestamp.

10 13. A system of claim 12, characterized in that the system includes a database arrangement coupled in communication with the server arrangement, wherein the log is to be maintained at the database arrangement.

14. A system of any one of claims 8 to 13, characterized in that the at  
15 least one bio-credential of the given user includes at least one of: a fingerprint of the given user, facial features of the given user, iris recognition of the given user, DNA genetic information of the given user.

15. A system of any one of claims 8 to 14, characterized in that the response message is received in an encrypted form.

20 16. A system of any one of claims 8 to 15, characterized in that the server arrangement is implemented to provide a background service that is configured to perform the aforesaid (i) to (iv), the background service being separate from the service.

17. A system of claim 16, characterized in that the background service  
25 is provided by a background service provider that is different from a service provider providing the service.

18. A computer program product comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a

computerized device comprising processing hardware to execute a method of any one of claims 1 to 7.

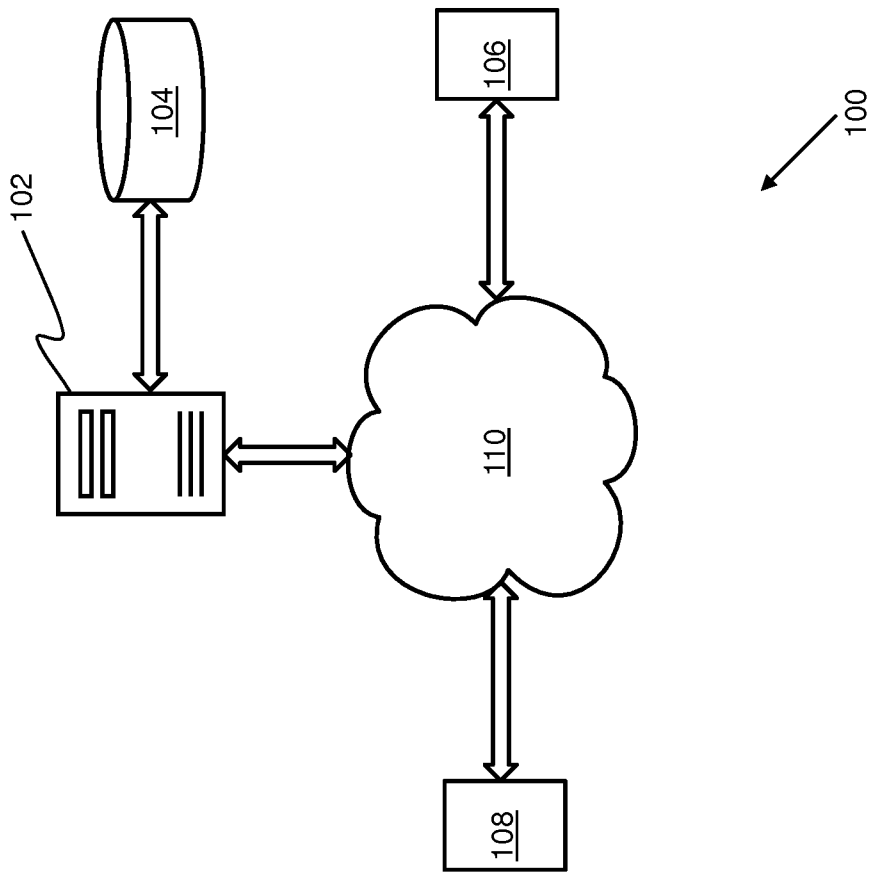


FIG. 1



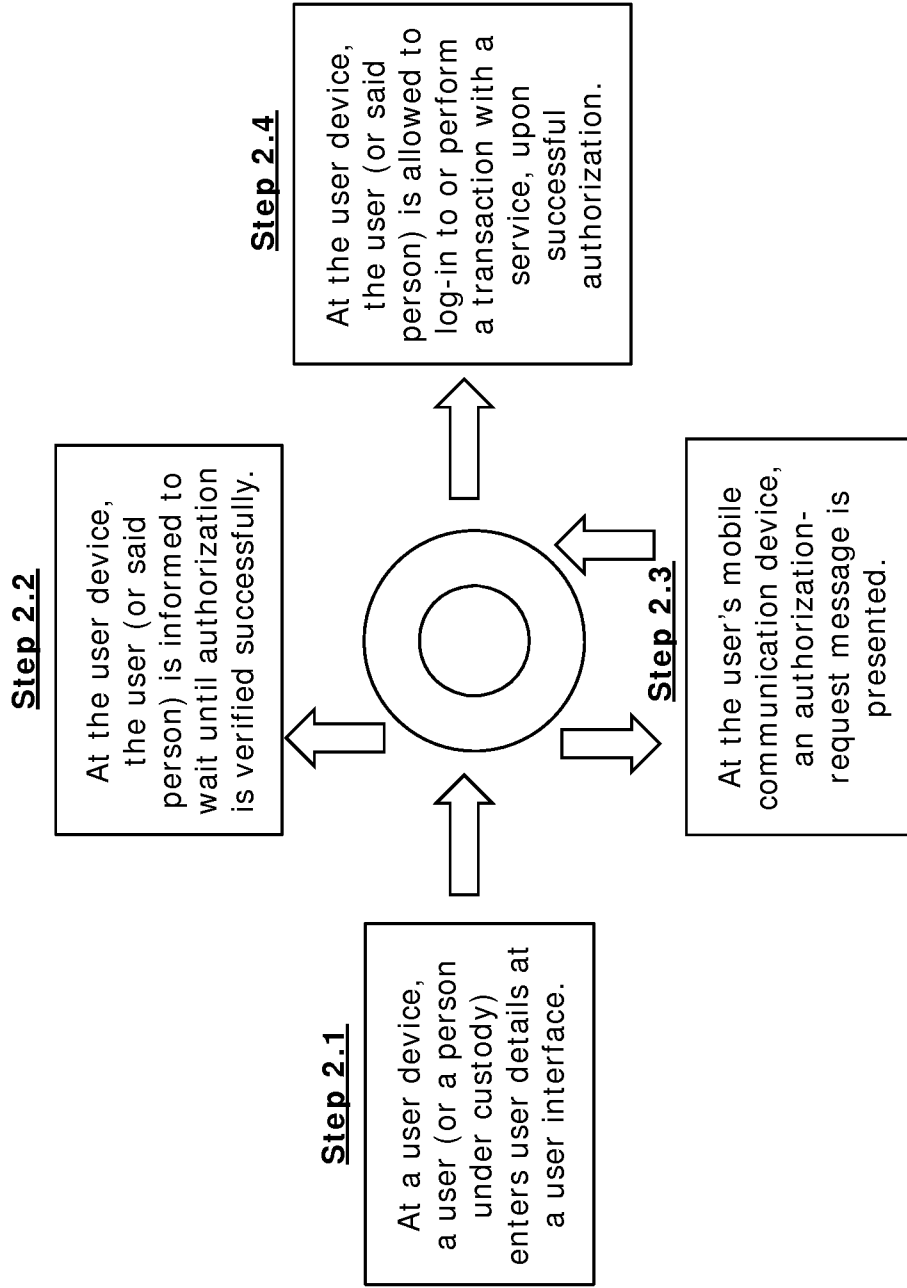


FIG. 2

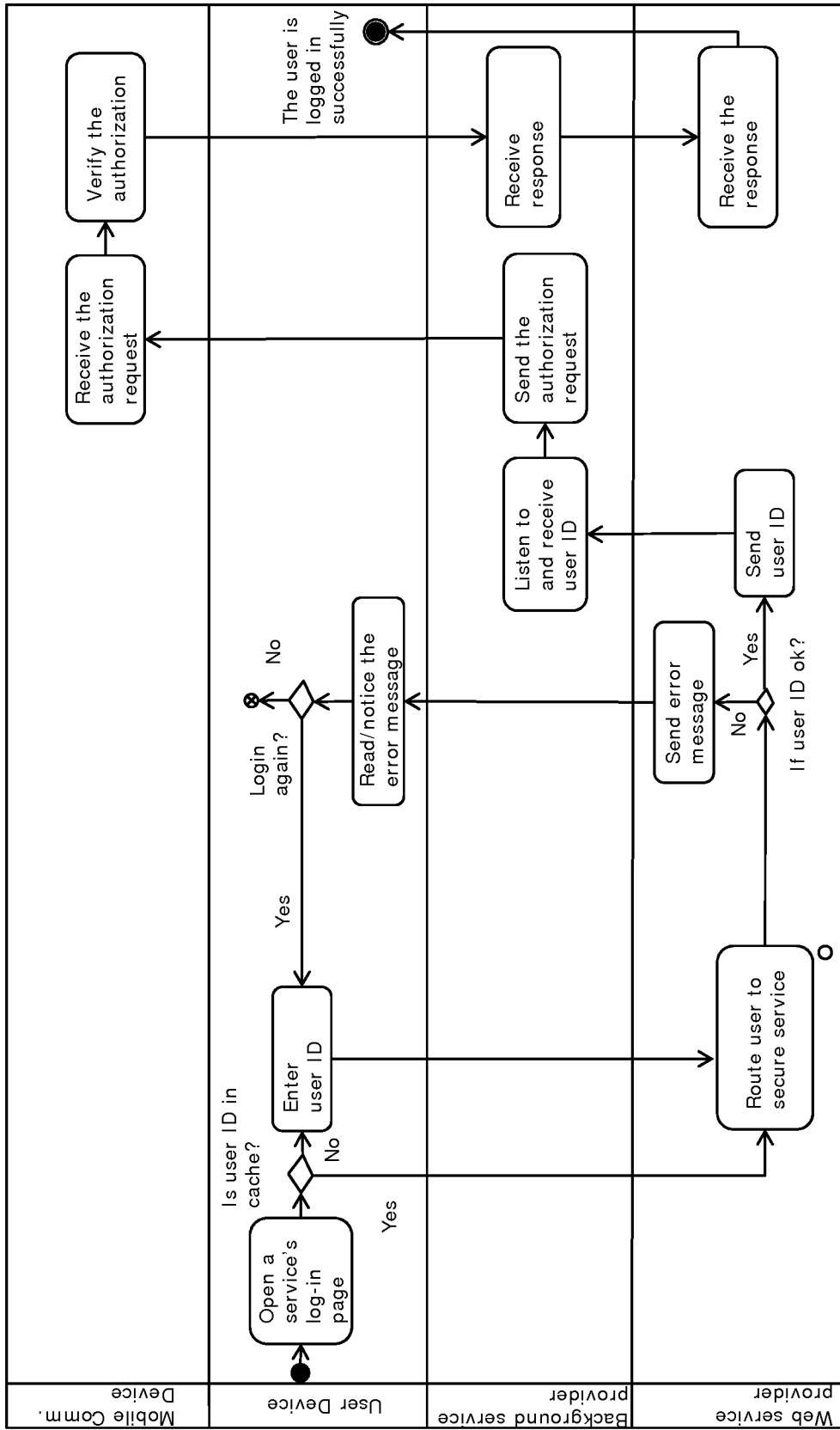


FIG. 3A

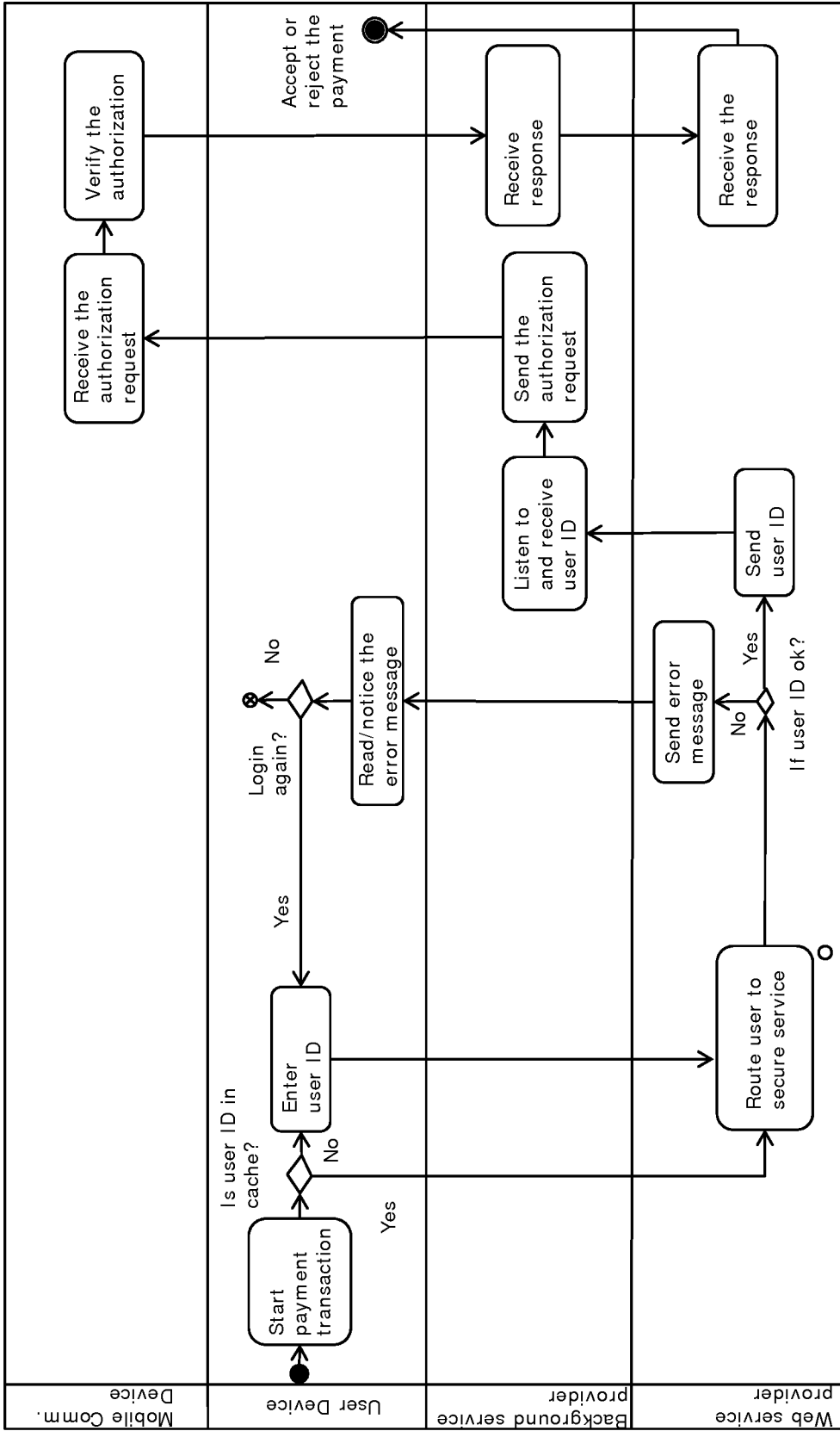


FIG. 3B

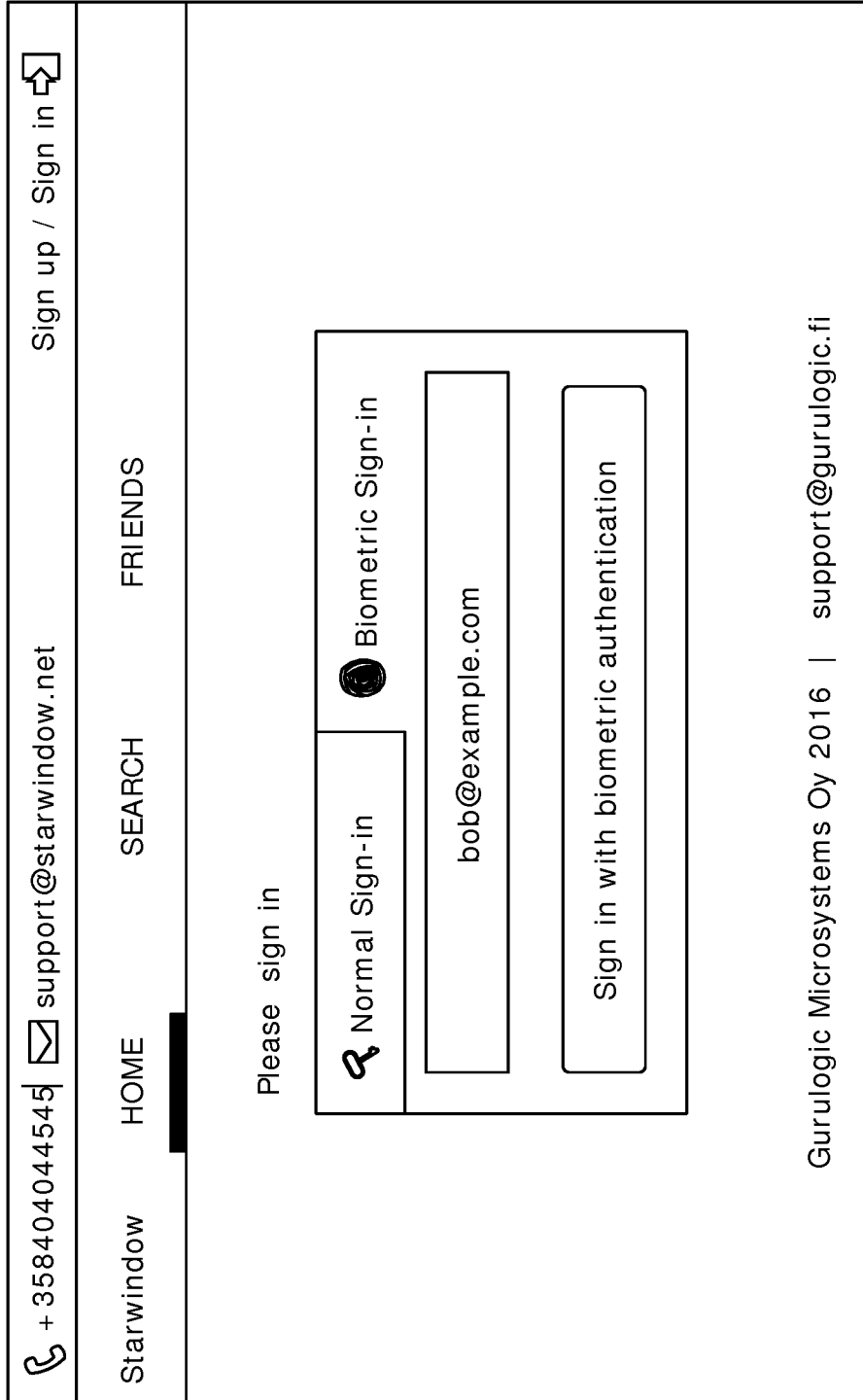


FIG. 4A

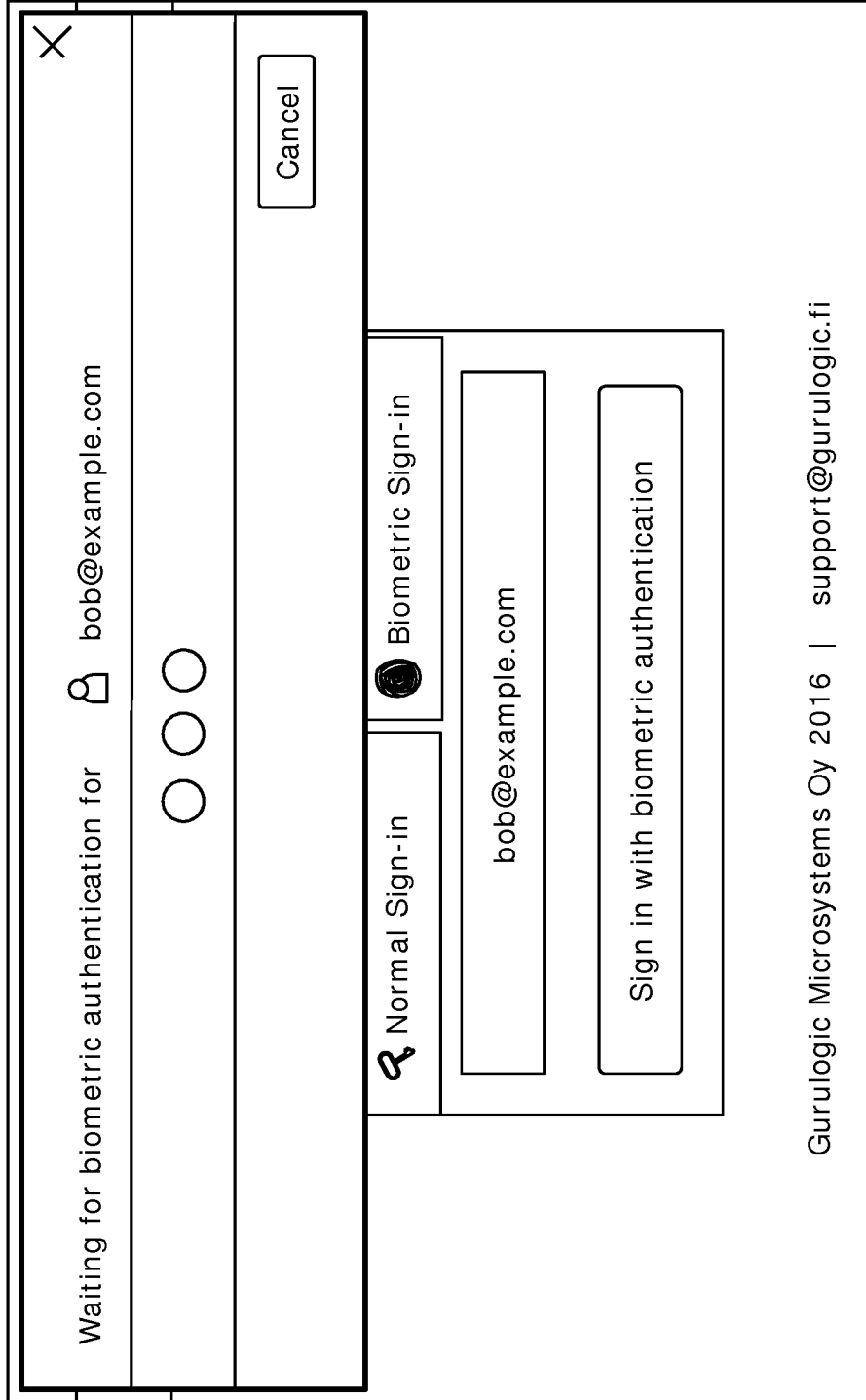


FIG. 4B

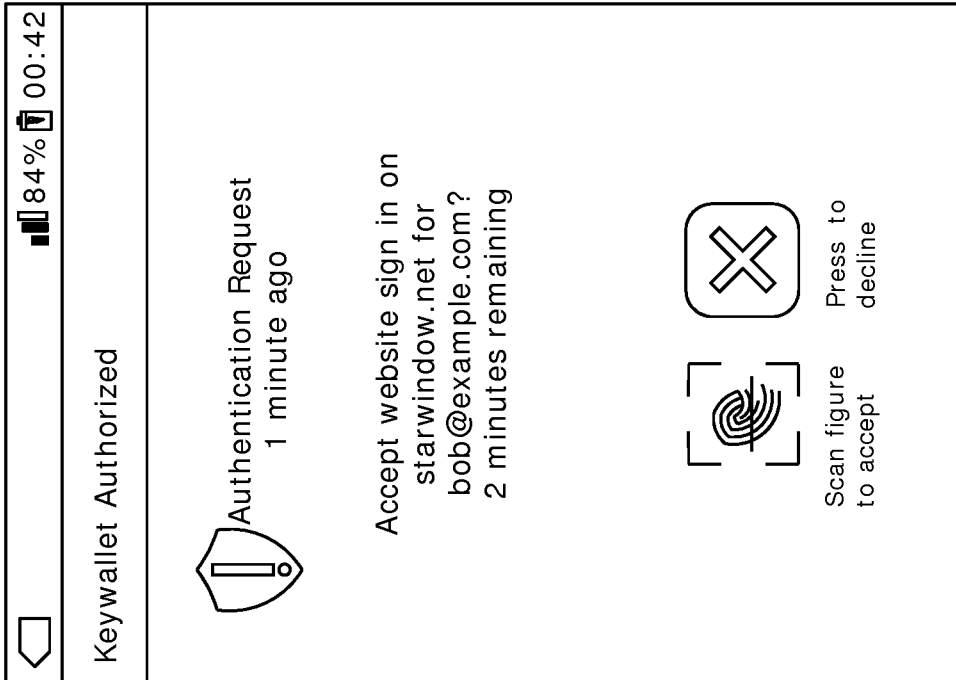


FIG. 4C


<p>+ 358404044545    support@starwindow.net</p>	<p>Starwindow</p>	<p>HOME</p>	<p>SEARCH</p>	<p>FRIENDS</p>	<p>bob@example.com / Log out</p>
<p>Gurulogic Microsystems Oy 2016   support@gurulogic.fi</p>					

FIG. 4D

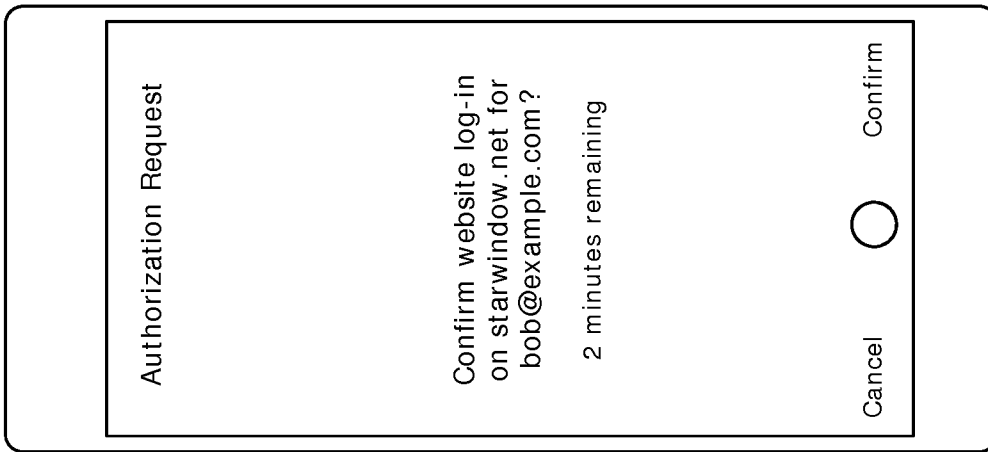


FIG. 5A

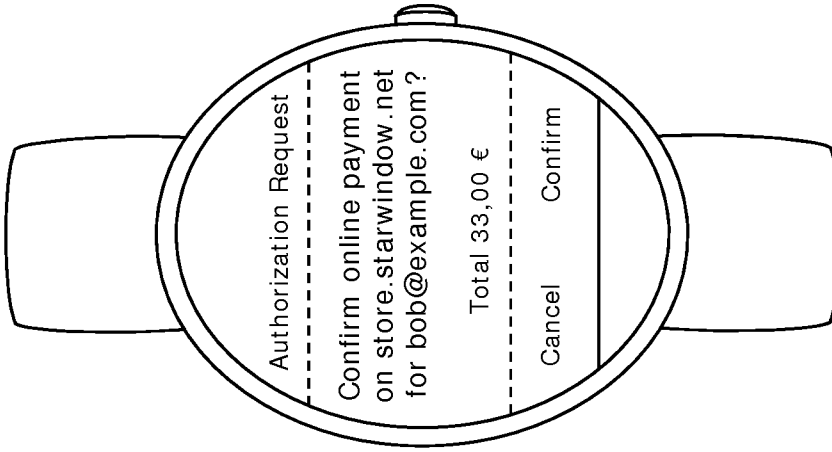


FIG. 5B



INTERNATIONAL SEARCH REPORT

International application No  
PCT/EP2017/025367

A. CLASSIFICATION OF SUBJECT MATTER  
INV. G06Q20/00  
ADD.  
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED  
Minimum documentation searched (classification system followed by classification symbols)  
G06Q

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Anonymous: "Multi-factor authentication - Wikipedia", 8 December 2016 (2016-12-08), XP055467270, Retrieved from the Internet: URL:https://en.wikipedia.org/w/index.php?title=Multi-factor_authentication&oldid=753692694 [retrieved on 2018-04-16] the whole document -----	1-18

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  16 April 2018	Date of mailing of the international search report  03/05/2018
--	--

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