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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 August 2007 (30.08.2007)

PCT

(10) International Publication Number
WO 2007/098509 A1

(51) International Patent Classification:
H04Q 7/32 (2006.01)

(21) International Application Number:
PCT/US2007/062816

(22) International Filing Date:
26 February 2007 (26.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/361,274 24 February 2006 (24.02.2006) US

(71) Applicant *(for all designated States except US)*: **QUALCOMM INCORPORATED** [US/US]; Attn: International Ip Administration, 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KENAGY, Jason B.** [US/US]; 3360 Dale Street, San Diego, California 92104 (US). **NIJDAM, Marc Edward** [NL/US]; 4971 Kensington Drive, San Diego, California 92116 (US). **BERNARD, Christophe** [US/US]; 6826 Beloit Avenue, San Diego, California 92111 (US).

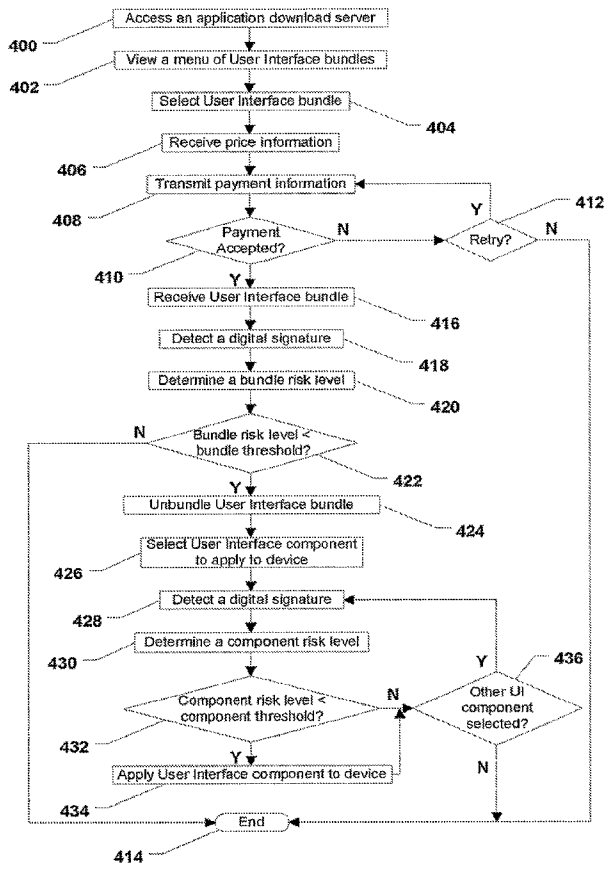
(74) Agent: **OGROD, Gregory D.**; Attn: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR DOWNLOADING USER INTERFACE COMPONENTS TO WIRELESS DEVICES



(57) Abstract: A method of processing a user interface component is provided and includes receiving one or more user interface components that can be communicated to a wireless device. A component risk level for each of the one or more user interface components is determined and assigned to each of the one or more user interface components. Each of the one or more user interface components can be digitally signed using an embedded risk code that indicates the assigned risk level. Further, the component risk level can be selected from a plurality of component risk levels. In a particular embodiment, the component risk level can be determined based on the type of the user interface component. Further, the component risk level can be determined based on a developer of the user interface component.

WO 2007/098509 A1

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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))*

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR DOWLOADING USER INTERFACE COMPONENTS TO WIRELESS DEVICES

BACKGROUND

I. *Field*

[0001] The present disclosure generally relates to user interfaces for wireless devices. More particularly, the disclosure relates to downloading user interface components to wireless devices.

II. *Description of Related Art*

[0002] Advances in technology have resulted in smaller and more powerful wireless devices. For example, there currently exist a variety of wireless devices, including mobile phones, personal digital assistants (PDAs), laptops, and paging devices that are small, lightweight, and easily carried by users. These devices may include the ability to transmit voice and/or data over wireless networks. Further, many such wireless devices provide significant computing capabilities, and as such, are becoming tantamount to small personal computers and hand-held PDAs.

[0003] Typically, these smaller and more powerful wireless devices are often resource constrained. For example, the screen size, the amount of available memory and file system space, and the amount of input and output capabilities may be limited by the small size of the device. Because of such severe resource constraints, it is can be desirable to maintain a limited size and quantity of software applications and other information residing on such wireless devices.

[0004] Some of these wireless devices utilize application programming interfaces (APIs) that are sometimes referred to as runtime environments and software platforms. The APIs can be installed onto a wireless device to simplify the operation and programming of such wireless devices by providing generalized calls for device resources. Further, some APIs can provide software developers the ability to create software applications that are executable on such wireless devices. In addition, APIs can provide an interface between a wireless device system hardware and the software applications. As such, the wireless device functionality can be made available to the software applications by allowing the software to make a generic call for a function thus not requiring the developer to tailor its source code to the individual hardware or device

on which the software is executing. Further, some APIs can provide mechanisms for secure communications between wireless devices, such as client devices and server systems, using secure cryptographic key information.

[0005] Examples of such APIs, some of which are discussed in more detail below, include those currently publicly available versions of the Binary Runtime Environment for Wireless® (BREW®) platform, developed by Qualcomm, Inc. of San Diego, California. The BREW® platform can provide one or more interfaces to particular hardware and software features found on wireless devices.

[0006] Further, the BREW® platform can be used in an end-to-end software distribution system to provide a variety of benefits for wireless service operators, software developers and wireless device manufacturers and consumers. One such currently available end-to-end software distribution system, called the BREW® solution developed by QUALCOMM Incorporated, includes logic distributed over a server-client architecture, wherein the server can perform billing, security, and application distribution functionality, and wherein the client can perform application execution, security and user interface functionality.

[0007] Some of the software applications that are developed to operate on the BREW® platform and that can be downloaded to wireless devices can include user interface components. After being downloaded to a wireless device, a user interface component can be executed to update or replace a previously existing user interface component, e.g., a background or a skin. Sometimes the user interface component can include one or more program bugs and executing the user interface component at the wireless device may render the wireless device inoperable.

[0008] Accordingly it would be advantageous to provide an improved system and method of downloading user interface components to wireless devices.

SUMMARY

[0009] A method of processing a user interface component is provided and includes receiving one or more user interface components that can be communicated to a wireless device. A component risk level for each of the one or more user interface components is determined and assigned to each of the one or more user interface components.

[0010] In a particular embodiment, each of the one or more user interface components is digitally signed using an embedded risk code that indicates the assigned risk level. Further, the component risk level can be selected from a plurality of component risk levels. In a particular embodiment, the component risk level can be determined based on the type of the user interface component. Further, the component risk level can be determined based on a developer of the user interface component. For example, a lower risk level can be assigned to each user interface component that is developed by an approved developer. On the other hand, a higher risk level can be assigned to each user interface component that is developed by an unapproved developer.

[0011] In a particular embodiment, the method further includes downloading the one or more user interface components to a wireless device. Moreover, the multiple user interface components can be bundled together in order to generate a user interface bundle and a bundle risk level for the user interface bundle can be determined. Particularly, the bundle risk level can be determined based on each component risk level of the user interface components within the user interface bundle. Also, the user interface bundle can be digitally signed. The user interface bundle can also be downloaded to the wireless device. In a particular embodiment, the method includes charging a fee to download the user interface bundle to the wireless device. Particularly, the user interface bundle can be downloaded to the wireless device via an over the air interface although cabled downloads are also possible.

[0012] In another embodiment, a method of obtaining user interface components at a wireless device is provided. The method includes accessing a download server and receiving a user interface bundle from the download server. Particularly, the user interface bundle can include a bundle risk level that is associated with loading the user interface bundle onto the wireless device.

[0013] In yet another embodiment, a wireless device is provided and includes a processor and a memory that is accessible by the processor. A user interface is stored within the memory and is executable by the processor. The memory further includes a user interface bundle embedded therein. Further, the user interface bundle includes a bundle risk level.

[0014] In still another embodiment, a system for downloading user interface components is provided and includes a security server and a stored application database

that is accessible to an application download server and the security server. A user interface bundle can be stored within the stored application database. Also, the user interface bundle comprises a plurality of user interface components and a bundle risk level that is associated with an assigned risk that is further associated with downloading the user interface bundle to a wireless device.

[0015] In yet still another embodiment, a computer program is provided and is embedded within a computer readable medium. The computer program includes instructions to receive one or more user interface components. Moreover, the computer program includes instructions to determine a component risk level for each of the one or more received user interface components. The component risk level indicates a risk that is associated with executing a user interface component at a wireless device. The computer program also includes instructions to assign each of the one or more user interface components a determined component risk level.

[0016] In still yet another embodiment, a computer program is provided and is embedded within a computer readable medium. Particularly, the computer program includes instructions to receive a user interface bundle. The user interface bundle includes a data item that indicates the security risk of unbundling the user interface bundle at a wireless device.

[0017] In another embodiment, a user interface for a wireless device is provided and includes a menu of risk level thresholds. A first risk level threshold can be selected from the menu and file bundles that have a risk level below the first risk level threshold can be received at the wireless device.

[0018] In yet another embodiment, a user interface for a computer is provided and includes a menu of risk level thresholds. A first risk level threshold can be selected from the menu. The first risk level can be assigned to a file before the file is downloaded to a wireless device and executed at the wireless device.

[0019] Other aspects, advantages, and features of the present disclosure will become apparent after review of the entire application, including the following sections: Brief Description of the Drawings, Detailed Description, and the Claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] The aspects and the attendant advantages of the embodiments described herein will become more readily apparent by reference to the following detailed description when taken in conjunction with the accompanying drawings wherein:

[0021] FIG. 1 is a general diagram of a particular embodiment of a system providing communications between a wireless device and a server;

[0022] FIG. 2 is a general diagram that illustrates further details of the particular embodiment of the system of FIG. 1;

[0023] FIG. 3 is a flowchart illustrating a method of providing user interface components to a wireless device;

[0024] FIG. 4 is a flowchart illustrating a method of receiving user interface components at a wireless device;

[0025] FIG. 5 is a diagram of a wireless device showing a first user interface;

[0026] FIG. 6 is a diagram of the wireless device showing a second user interface;

[0027] FIG. 7 is a diagram of the wireless device showing a third user interface;

[0028] FIG. 8 is a diagram of a computer showing a first user interface;

[0029] FIG. 9 is a diagram of the computer showing a second user interface; and

[0030] FIG. 10 is a diagram of the computer showing a third user interface.

DETAILED DESCRIPTION

[0031] The word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments. Further, many embodiments are described in terms of sequences of actions to be performed by, for example, elements of a wireless device. It will be recognized that various actions described herein could be performed by specific circuits, e.g., application specific integrated circuits (ASICs), by program instructions being executed by one or more processors, or by a combination of both.

[0032] Further, the embodiments described herein can additionally be considered to be embodied entirely within any form of computer readable storage medium having stored therein a corresponding set of computer instructions that upon execution would cause an associated processor to perform the functionality described herein. Thus, various

aspects of the disclosure may be embodied in a number of different forms, all of which have been contemplated to be within the scope of the claimed subject matter. In addition, for each of the embodiments described herein, the corresponding form of any such embodiments may be described herein as, for example, "logic configured to" perform a certain action or "code operable to" perform the described action. The following detailed description describes methods, systems, software and apparatus used in connection with one or wireless devices.

[0033] In one or more embodiments, a wireless device may utilize a runtime environment such as, a version of the Binary Runtime Environment for Wireless® (BREW®) platform developed by QUALCOMM, Inc., of San Diego, California. In at least one embodiment in the following description, the system used to provide communications between wireless devices and servers is implemented on a wireless device executing a runtime environment, such as the current version of the BREW® platform. However, one or more embodiments of the system used to provide communications between wireless devices and servers are suitable for use with other types of runtime environments that, for example, operate to control the execution of applications on wireless devices.

[0034] FIG. 1 illustrates a block diagram of an exemplary, non-limiting embodiment of a system 100, that may perform loading, reloading, and deletion of software application components on a wireless device, such as wireless telephone 102. The wireless telephone 102 communicates across a wireless network 104 with at least one application download server 106. Further, the application download server 106 can selectively transmit one or more software applications and components to one or more wireless devices across a wireless communication portal or other node that has data access to the wireless network 104.

[0035] As illustrated in FIG. 1, the wireless device can be a wireless telephone 102, a personal digital assistant 108, a pager 110, or a separate computer platform 112 that has a wireless communication portal. In a particular embodiment, the pager 110 can be a two-way text pager. Further, in an alternative embodiment, the wireless device can have a wired connection 114 to a network or the Internet. The exemplary, non-limiting system can include any form of a remote module including a wireless communication portal, including without limitation, wireless modems, PCMCIA cards, personal

computers, access terminals, telephones with or without a display or keypad, or any combination or sub-combination thereof.

[0036] As depicted in FIG. 1, the application download server 106 is coupled to a network 116 with other computer elements in communication with the wireless network 104. The system 100 includes a security server 120 and a stand-alone server 122, and each server can provide separate services and processes to the wireless devices 102, 108, 110, 112 across the wireless network 104. Further, as indicated in FIG. 1, the system 100 also includes at least one stored application database 118 that stores software applications that can be downloaded to the wireless devices 102, 108, 110, 112. Different embodiments are contemplated that locate logic to perform secure communications at any one or more of the application download server 106, the security server 120 and the stand-alone server 122.

[0037] In a particular embodiment, one or more user interface components 124 can be developed on a computer, e.g., the computer 112, and uploaded to the network 116 via the wireless network 104 or wired connection 114. Further, the user interface component 124 can be assigned a security risk level and signed with a digital signature that includes an embedded code that represents the risk level for the user interface component 124. In a particular embodiment, the risk level represents a risk of operating system damage associated with executing the user interface component 124 at a wireless device to which the user interface component 124 is downloaded. Thereafter, multiple digitally signed user interface components 124 can be bundled together to produce a user interface bundle 126 that can be stored within the stored applications database 118. The user interface bundle 126 can also be assigned a security risk level and signed with a digital signature that includes the risk level for the user interface bundle 126. Particularly, the risk level for the user interface bundle 126 represents a risk of system damage associated with unbundling the user interface bundle 126 at a wireless device to which the user interface bundle 126 is downloaded.

[0038] In an illustrative embodiment, the user interface component 124 can be a graphical user interface component, such as a graphical icon, a virtual button, a skin, a background, a font package, or a graphical menu that is linked to a physical user interface component, such as a keypad button, a keyboard button, or a mouse. The user interface component 124 can also be a collection of graphical user interface

components, e.g., an entire graphical user interface. The user interface component 124 can also be a graphical user interface component such as a touch screen component that can be selected by touching the display screen of the wireless device with a finger or a stylus. Also, the user interface component 124 can be an entire touch screen user interface. Further, in another illustrative embodiment, the user interface component 124 can be a voice user interface component, such as a voice command linked to a particular function, such as dialing a telephone number. Moreover, the user interface component 124 can be an entire voice user interface having multiple voice commands and corresponding actions. In a particular embodiment, the user interface component 124 can upgrade an existing user interface component 124 at a wireless device, replace a previously loaded user interface component 124, or the user interface component 124 can be a new installation of a user interface component 124 for the wireless device.

[0039] In a particular embodiment, the risk levels for the user interface components 124 can be determined based on the type of user interface component 124, the type of wireless device to which the user interface component 124 is downloaded, and the extent of the changes to the user interface caused by executing the user interface component 124 at the wireless device. For example, simple font packages can be assigned a low risk, while a user interface component 124, such as a background or skin can be assigned a medium risk. Further, a more pervasive user interface component 124 such as an entirely new user interface that changes the functionality of the wireless device in addition to the appearance of the wireless device can be assigned a high risk.

[0040] Additionally, the risk levels for the user interface components 124 can be determined based on whether the developer is an approved or trusted developer, i.e., a developer that has a proven track record of producing user interface components 124 that work as intended, execute without problems, and do not prevent the wireless device from operating properly. Further, a developer that is trusted is deemed to be privileged to develop user interface components that can be downloaded to wireless devices. In a particular embodiment, a developer can gain approval by paying a fee. Also, in a particular embodiment, the risk levels can be assigned by a particular wireless device manufacturer, an industry group, or some other group.

[0041] In a particular embodiment, the risk may be automatically assigned for a developer without the developer's input or consent. Also, the risk can be assigned

based on how long a particular developer has been involved in a particular project. For example, developers that joined the development earlier in the development path may be assigned less risk than new or upcoming developers. Further, the risk can be assigned based on when a component is developed or when a component is to be delivered. Additionally, as a particular user interface component or bundle is developed the risk level may change depending on the various developers that have "handled" the particular user interface component or bundle. Risk levels for subsequent handlers may be automatically determined.

[0042] Accordingly, a particular user interface component 124 can have one of the following exemplary, non-limiting risk levels: low and trusted, low and unapproved, medium and trusted, medium and unapproved, high and approved, and high and unapproved. In a particular embodiment, the risk level for a user interface bundle 126 is determined based on a combination of the risk levels of the individual user interface components in the bundle. The digital signatures ensure that the risk levels are able to be controlled and enforced. Further, the digital signatures prevent tampering of the user interface components once they are assigned a risk level and digitally signed.

[0043] In FIG. 2, a block diagram is shown that more fully illustrates the system 100, including the components of the wireless network 104 and interrelation of the elements of the system 100. The system 100 is merely exemplary and can include any system whereby remote modules, such as the wireless devices 102, 108, 110, 112 communicate over-the-air between and among each other and/or between and among components connected via a wireless network 104, including, without limitation, wireless network carriers and/or servers. The application download server 106 and the stored application database 118, along with any other servers, such as server 120, are compatible with wireless communication services and can communicate with a carrier network 200 through a data link, such as the Internet, a secure LAN, WAN, or other network. In an illustrative embodiment, the server 120 contains a server security module 128 that further contains logic configured to provide for secure communications over the carrier network 200. In a particular embodiment, the server security module 128 can operate in conjunction with a client security module located on a wireless device, such as wireless devices 102, 108, 110, 112, to provide secure communications. Additionally, the server security module 128 can assign risk levels to user interface components 124 sent to the

security server 120. Also, the server security module 128 can assign risk levels to the user interface bundles 126.

[0044] The carrier network 200 controls messages (sent as data packets) sent to a mobile switching center ("MSC") 202. The carrier network 200 communicates with the MSC 202 by a network, such as the Internet and/or POTS ("plain ordinary telephone system"). Typically, the network connection between the carrier network 200 and the MSC 202 transfers data, and the POTS transfers voice information. The MSC 202 is connected to multiple base transceiver stations ("BTS") 204. The MSC 202 can be connected to the BTS 204 by both a data network and/or Internet for data transfer and POTS for voice information. The BTS 204 ultimately broadcasts messages wirelessly to the wireless devices, such as to wireless telephone 102, by the short messaging service ("SMS"), or other over-the-air methods known in the art.

[0045] The wireless device 102 has a computer platform 206 that can receive and execute software applications transmitted from the application download server 106. In an illustrative embodiment, the computer platform 206 may be implemented as an application-specific integrated circuit (ASIC 208), a processor, microprocessor, logic circuit, or other data processing device. The ASIC 208 can be installed at the time of manufacture of the wireless device. Further, the ASIC 208 or other processor can execute an application programming interface (API) 210 layer that interfaces with resident programs in the memory 212 of the wireless device. In a particular embodiment, the API 210 layer includes a set of APIs provided by the Binary Runtime Environment for Wireless® (BREW®) platform. The memory 212 can be comprised of read-only or random-access memory (ROM or RAM), EEPROM, flash memory, or any other memory suitable for computer platforms.

[0046] The API 210 also includes a client security module 214 containing logic configured to provide for secure communications over the carrier network 200. In a particular embodiment, the client security module 214 can operate in conjunction with the server security module 128 to provide secure communications. Additionally, the client security module 214 can detect and decode the digital signatures of user interface components 124 and user interface bundles 126 downloaded to the wireless device and can determine the assigned risk levels of a user interface bundle 126 and each of the user interface components 124.

[0047] Also, the client security module 214 can compare the risk level for each user interface bundle 126 and the risk level for each user interface component 124 to a predetermined threshold level, e.g., a threshold level for specific user interface components 124 or a global threshold level for a user interface bundle 126, in order to determine whether the risk level is below a preset threshold. If the risk level for the user interface bundle 126 is below the bundle threshold level, the user interface bundle 126 is unbundled to produce multiple user interface components 124. Further, if the risk level for a user interface component 124 is below the component threshold level, each user interface component 124 can be executed at the wireless device. On the other hand, if the risk level for a user interface component 124 is above the component threshold level the user interface component 124 can be deleted, or otherwise removed, from the wireless device.

[0048] As illustrated in FIG. 2, the computer platform 206 can further include a local database 216 that can hold applications not actively used in memory 212. In an illustrative embodiment, the local database 216 is stored within a flash memory cell, but it can be stored within any secondary storage device as known in the art, such as magnetic media, EEPROM, optical media, tape, or floppy or hard disk. A wireless device, for example, the wireless telephone 102, can download one or more software applications, such as games, news, stock monitors, and the like, from the application download server 106. Further, the wireless device can store the downloaded applications in the local database 216, when not in use, and can load stored resident applications from the local database 216 to memory 212 for execution by the API 210 when desired by the user. Further, communications over the wireless network 104 may be performed in a secure manner, at least in part, due to the interaction and operation of the client security module 214 and the server security module 128.

[0049] Referring to FIG. 3, a method of providing user interface components to a wireless device is shown and commences at block 300 wherein a security server receives a user interface component, e.g., from a software developer. At block 302, a server security module within a security server determines a component risk level for the user interface component. Thereafter, at block 304, the server security module assigns the determined component risk level to the user interface component. Moving to block 306, the server security module digitally signs the user interface component. In

a particular embodiment, the digital signature can prevent tampering of the risk level and the user interface component.

[0050] Continuing to block 308, the server security module combines plural user interface components together to create a user interface bundle. At block 310, the server security module determines a bundle risk level for the user interface bundle. Then, at block 312, the server security module assigns the determined bundle risk level to the user interface bundle. At block 314, the server security module digitally signs the user interface bundle, in an illustrative embodiment, using an embedded risk code that indicates the assigned risk level generated and stored with a data packet associated with the user interface bundle to be deployed to a wireless device.

[0051] Proceeding to block 316, the security server stores the digitally signed user interface bundle in the stored applications database. Next, at block 318, the application download server presents user interface bundle information to a user via the wireless device. In a particular embodiment, the application download server presents a menu of digitally signed user interface bundles and information related to each digitally signed user interface bundle. In a particular embodiment, the information includes the bundle risk level for the user interface bundle, the component risk level for each user interface component that is included in the user interface bundle, and the type of each user interface component that is included in the user interface bundle.

[0052] Still referring to FIG. 3, at block 320, the application download server receives a request for a user interface bundle from a wireless device. In a particular embodiment, the request from the wireless device is received at the application download server via an over the air interface. At block 322, the application download server indicates the cost of the user interface bundle to the wireless device. At block 324, the application download server receives a purchase request from the wireless device. Moving to decision step 326, the application download server 106 determines whether payment information is received from the wireless device. If not, the method ends at state 328. On the other hand, if payment information is received from the wireless device, the method proceeds to decision step 330 and the application download server determines whether the payment from the wireless device is approved. If the payment is not approved, the method continues to block 332 and the application download server

indicates to the wireless device that the payment is not approved. The method then returns to decision step 326 and continues as described herein.

[0053] At decision step 330, if the application download server approves the user payment, the logic proceeds to block 334 and the application download server indicates to the wireless device that the payment from the wireless device is approved. Next, at block 336, the application download server downloads the user interface bundle to the wireless device. In a particular embodiment, the user interface bundle is downloaded to the wireless device via an over the air interface. The method of downloading the user interface bundle with an assigned risk level from an application download server ends at state 328.

[0054] Referring now to FIG. 4, a method of receiving user interface components having assigned risk levels at a wireless device is shown and commences at block 400. At block 400, a wireless device accesses the application download server. In a particular embodiment, the wireless device can communicate with the application download server via an over the air interface. Next, at block 402, a user of the wireless device can view a menu of user interface bundles that are available at the application download server. At block 404, using the wireless device, the user can select a user interface bundle to be downloaded by the application download server. At block 406, the wireless device receives price information related to the user interface bundle.

[0055] Moving to block 408, the wireless device can transmit payment information to the application download server. Thereafter, at decision step 410, the application download server indicates to the wireless device whether the payment is accepted. If the payment is not accepted, the method continues to decision step 412 and queries the user via the wireless device as to whether the user would like to retry payment. If so, the method returns to block 408 and new payment information is transmitted to the application download server. The method then continues as described herein.

[0056] At decision step 412, if the user does not want to retry payment, the method ends at state 414. Returning to decision step 410, if payment is accepted, the wireless device receives the user interface bundle at block 416. Moving to block 418, a digital signature associated with the user interface bundle is detected and decoded. At block 420, a bundle risk level is determined, such as by reading the embedded risk level code assigned by the security server. Continuing to decision step 422, the wireless device

compares the bundle risk level to a bundle risk level threshold in order to determine whether the bundle risk level is acceptable, i.e., less than the bundle threshold. If the bundle risk level is not less than the bundle threshold, the risk level is too high so the bundle is rejected and the method ends at state 414.

[0057] Conversely, if the bundle risk level is less than the bundle threshold, the method moves to block 424 and the user interface bundle is accepted and unbundled to produce multiple user interface components. At block 426, the wireless device detects the selection of one or more user interface components to be applied to the wireless device. In another embodiment, the wireless device can automatically determine which user interface components to be applied to the wireless device. Next, at block 428, a digital signature associated with the user interface component is detected and decoded. At block 430, a component risk level is determined for the user interface component. Proceeding to decision step 432, the wireless device compares the component risk level to a component risk level threshold in order to determine whether the component risk level is acceptable, i.e., less than the component threshold. In a particular embodiment, the risk level thresholds can be set by a wireless device manufacturer. Also, the risk level thresholds can be set by a user of the wireless device.

[0058] If the component risk level is less than the component risk level threshold, the component is accepted and the method moves to block 434 where the user interface component is applied to the wireless device. In a particular embodiment, the user interface component may be an upgrade to an existing user interface. In another embodiment, the user interface component is a new component that is applied to the wireless device. The logic then moves to decision step 436.

[0059] Returning to decision step 432, if the component risk level is not less than the component threshold, the method moves to decision step 436. At decision step 436, the wireless device determines whether there is another user interface component selected for application to the wireless device. If so, the method returns to block 428 and continues as described above. If no other user interface components are available, the method ends at state 414. In a particular embodiment, the decision to unbundle a user interface bundle and the decision to apply a user interface component to the wireless device can be made by logic within the wireless device without the user's input or knowledge. Otherwise, the user can select set a threshold for each decision. Also, the

decision to unbundle and the decision to apply can be based on the cause of the download, e.g., was the download automatic or requested by a user.

[0060] FIG. 5 shows a wireless device, generally designated 500. As depicted in FIG. 5, the wireless device includes a display 502 and a keypad 504. FIG. 5 indicates that a download/execution threshold menu 506 can be presented to a user via the display 502. A user can scroll through the download/execution threshold menu 506 using the keypad 504 and then, using the keypad 504 or a soft button 508 select a particular threshold. In a particular embodiment, the threshold can apply to downloading user interface bundles to the wireless device 500 and to executing user interface components at the wireless device 500. Alternatively, a user can select a first threshold for downloading user interface bundles to the wireless device 500 and a second threshold for executing user interface components at the wireless device 500.

[0061] FIG. 6 shows that a menu of user interface bundles 600 can be displayed at the wireless device 500. A user can scroll through the menu of user interface bundles 600 using the keypad 504 and then, using the keypad 504 or a first soft button 602, the user can select a particular user interface bundle to unbundle at the wireless device 500. Also, the user can select a particular user interface bundle from the menu 600 and toggle second soft button 604 to cause the particular user interface bundle to be downloaded to the wireless device 500. Also, as indicated in FIG. 7, a menu of user interface components 700 can be displayed at the wireless device 500. A user can scroll through the menu of user interface components 700 using the keypad 504 and then, using the keypad 504 or a first soft button 702 select a particular user interface component to execute at the wireless device 500. The user can also download a particular user interface component presented at via the menu 700 by toggling a second soft button 704.

[0062] FIG. 8 shows a computer, generally designated 800. As depicted in FIG. 8, the computer includes a display 802, a keyboard 804, and a mouse 806. FIG. 8 indicates that a user interface component menu 808 can be presented to a user via the display 802. A user can select one or more user interface components from the menu 808 by clicking on a first soft button 810 with the mouse 806. Further, the user can assign a risk level to a selected user interface component by clicking on a second soft button 812 to bring up a risk level menu. The user can also upload a selected user interface component to an

application download server by toggling on a third soft button 814. Additionally, the user can bundle multiple selected user interface components by clicking on a fourth soft button 816.

[0063] FIG. 9 shows a risk level menu 900 that can be presented at the computer. A user can select a risk level by clicking on a select button 902 with the mouse. Referring to FIG. 10, a user interface bundle menu 1000 can be presented to a user via the display 802. A user can select assign a risk level to a particular user interface bundle by selecting the particular user interface bundle from the menu 1000 and then, clicking on a first soft button 1002 with a mouse 804. When the first soft button 1002 is toggled, the risk level menu 900 is, again, presented to the user at the computer 800. The user can also upload a selected user interface bundle to an application download server by clicking, or otherwise toggling, a second soft button 1004 presented to the user at the computer 800.

[0064] With the configuration of structure described above, the system and method of downloading user interface components to wireless devices provides a method for a wireless device to determine a risk level associated with executing one or more user interface components prior to execution. Accordingly, user interface components that appear to present a greater security risk can be rejected by the wireless device.

[0065] Those of skill would further appreciate that the various illustrative logical blocks, configurations, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, configurations, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present disclosure.

[0066] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module

may reside in RAM memory, flash memory, ROM memory, PROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor such that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in a wireless device or a user terminal. In the alternative, the processor and the storage medium may reside as discrete components in a wireless device or user terminal.

[0067] The previous description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present disclosure. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from the spirit or scope of the disclosure. Thus, the present disclosure is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features as defined by the following claims.

CLAIMS

WHAT IS CLAIMED IS:

1. A method of processing a user interface component, the method comprising:

receiving one or more user interface components to be communicated to a wireless device;

determining a component risk level for each of the one or more user interface components; and

assigning a determined component risk level to each of the one or more user interface components.

2. The method of claim 1, further comprising digitally signing each of the one or more user interface components using an embedded risk code that indicates the assigned risk level.

3. The method of claim 1, wherein the component risk level is selected from a plurality of component risk levels.

4. The method of claim 1, wherein the component risk level is determined at least partially based on the type of the user interface component.

5. The method of claim 1, wherein the component risk level is determined at least partially based on a developer of the user interface component.

6. The method of claim 5, wherein a lower risk level is assigned to each user interface component that is developed by an approved developer.

7. The method of claim 5, wherein a higher risk level is assigned to each user interface component that is developed by an unapproved developer.

8. The method of claim 1, further comprising downloading the one or more user interface components to a wireless device.

9. The method of claim 1, further comprising bundling multiple user interface components to generated a user interface bundle.

10. The method of claim 9, further comprising determining a bundle risk level for the user interface bundle.

11. The method of claim 10, wherein the bundle risk level is determined at least partially based on each component risk level of user interface components within the user interface bundle.

12. The method of claim 11, further comprising digitally signing the user interface bundle.

13. The method of claim 12, further comprising downloading the user interface bundle to the wireless device.

14. The method of claim 13, further comprising charging a fee to download the user interface bundle to the wireless device.

15. The method of claim 14, wherein the user interface bundle is downloaded to the wireless device via an over the air interface.

16. A method of obtaining user interface components at a wireless device, comprising:

accessing a download server; and

receiving a user interface bundle from the download server, the user interface bundle including a bundle risk level associated with loading the user interface bundle onto the wireless device.

17. The method of claim 16, further comprising selecting the user interface bundle from a menu of available user interface bundles prior to receiving the user interface bundle.

18. The method of claim 17, further comprising detecting and decoding the bundle digital signature of the user interface bundle received from the download server.

19. The method of claim 18, further comprising determining the bundle risk level after decoding a bundle digital signature of the user interface bundle.

20. The method of claim 19, further comprising comparing the bundle risk level to a bundle threshold.

21. The method of claim 20, further comprising unbundling the user interface bundle to produce a plurality of user interface components after comparing the bundle risk level to the bundle threshold.

22. The method of claim 21, wherein each of the plurality of user interface components is selected from the group consisting of a graphical user interface component, a voice user interface component, and a touch screen user interface component.

23. The method of claim 21, wherein each of the plurality of user interface components has a component digital signature and a component risk level associated with loading the user interface component onto the wireless device.

24. The method of claim 23, further comprising detecting the component digital signature of at least one of the user interface component.

25. The method of claim 24, further comprising comparing the component risk level to a component risk level threshold.

26. The method of claim 25, further comprising selectively applying one or more of the plurality of user interface components to the wireless device at least partially based on a result of comparing the component risk level to the component threshold.

27. A wireless device, comprising:

a processor;

a memory accessible by the processor;

a user interface stored within the memory and executable by the processor;

and

a user interface bundle embedded within the memory, the user interface bundle having a bundle risk level.

28. The wireless device of claim 27, further comprising a display coupled to the processor, wherein a menu of user interface component bundles is presented to a user via the display before a selected user interface bundle is downloaded to the wireless device and stored within the memory.

29. The wireless device of claim 28, wherein the user interface bundle comprises a plurality of user interface components.

30. The wireless device of claim 29, wherein each user interface component includes a component risk level associated with execution of the user interface component by the processor.

31. A system for downloading user interface components, comprising:

a security server;

a stored application database accessible to an application download server; and

at least one user interface bundle stored within the stored application database, wherein the user interface bundle comprises a plurality of user interface components and a bundle risk level associated with an assigned risk associated with downloading the user interface bundle to a wireless device.

32. The system of claim 31, wherein each of the plurality of user interface components includes an assigned component risk level associated with executing the user interface component at the wireless device.

33. The system of claim 32, further comprising a security server coupled to the stored application database and a server security module embedded within the security server, the server module including a first computer program, the first computer program including instructions to receive at least one of the plurality of user interface components.

34. The system of claim 33, further comprising an application download server and second computer program within the application download server, the computer program comprising instructions to communicate one or more digitally signed user interface components to a wireless device.

35. A computer program embedded within a computer readable medium, the computer program comprising:

instructions to receive one or more user interface components;

instructions to determine a component risk level for each of the one or more received user interface components, the component risk level indicating a risk associated with executing a user interface component at a wireless device; and

instructions to assign each of the one or more user interface components a determined component risk level.

36. A computer program embedded within a computer readable medium, comprising:

instructions to receive a user interface bundle, the user interface bundle including a data item indicating the security risk of unbundling the user interface bundle at a wireless device.

37. An electronic device for processing a user interface component, comprising:

means for receiving one or more user interface components to be communicated to a wireless device;

means for determining a component risk level for each of the one or more user interface components; and

means for assigning a determined component risk level to each of the one or more user interface components.

38. An wireless device, comprising:

means for accessing a download server; and

means for receiving a user interface bundle from the download server, the user interface bundle including a bundle risk level associated with loading the user interface bundle onto the wireless device.

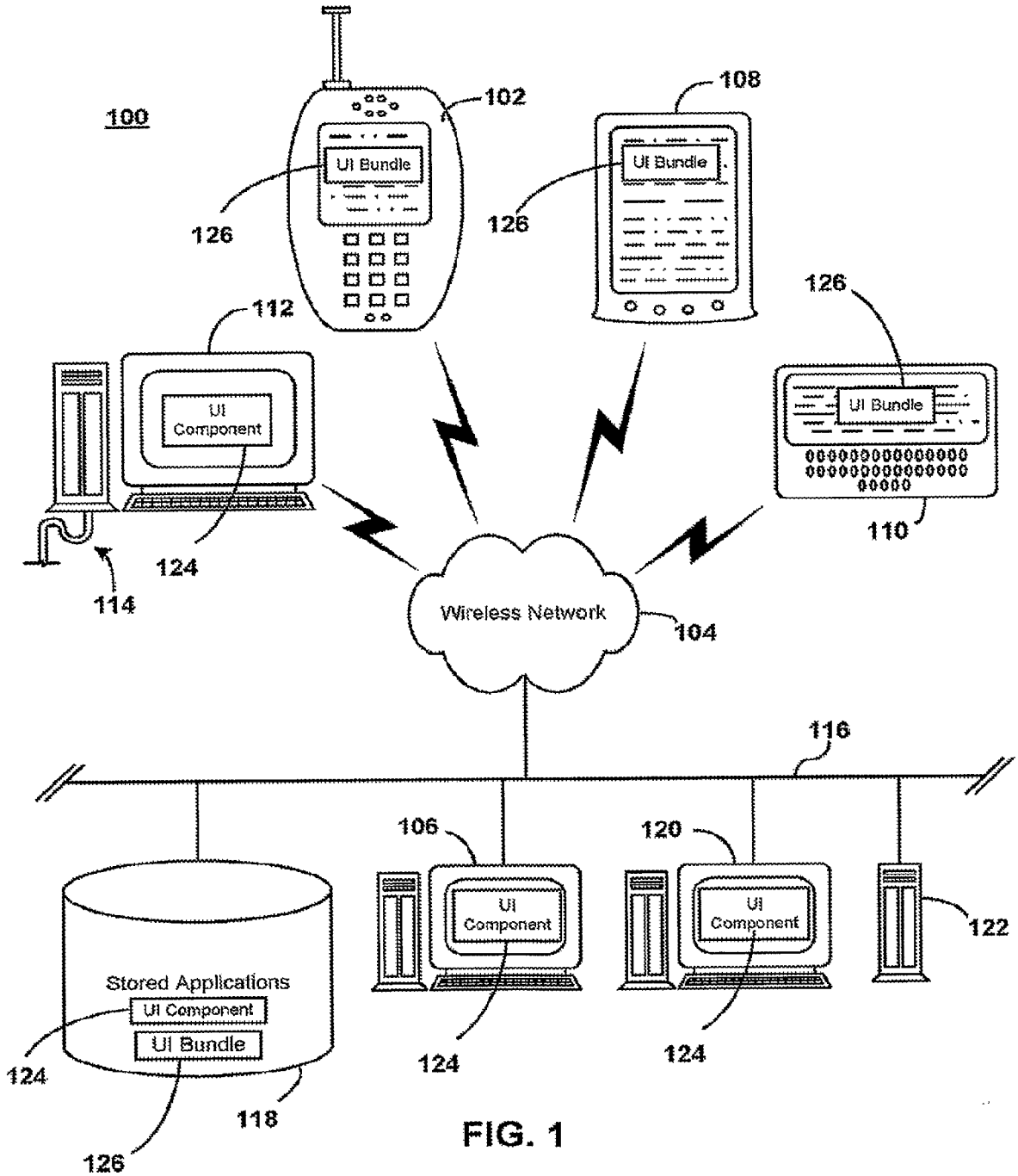

100
102
UI Bundle
126
108
UI Bundle
126
126
UI Bundle
110
112
UI Component
124
114
Wireless Network
104
116
106
UI Component
124
120
UI Component
124
122
Stored Applications
UI Component
UI Bundle
124
126
118

FIG. 1

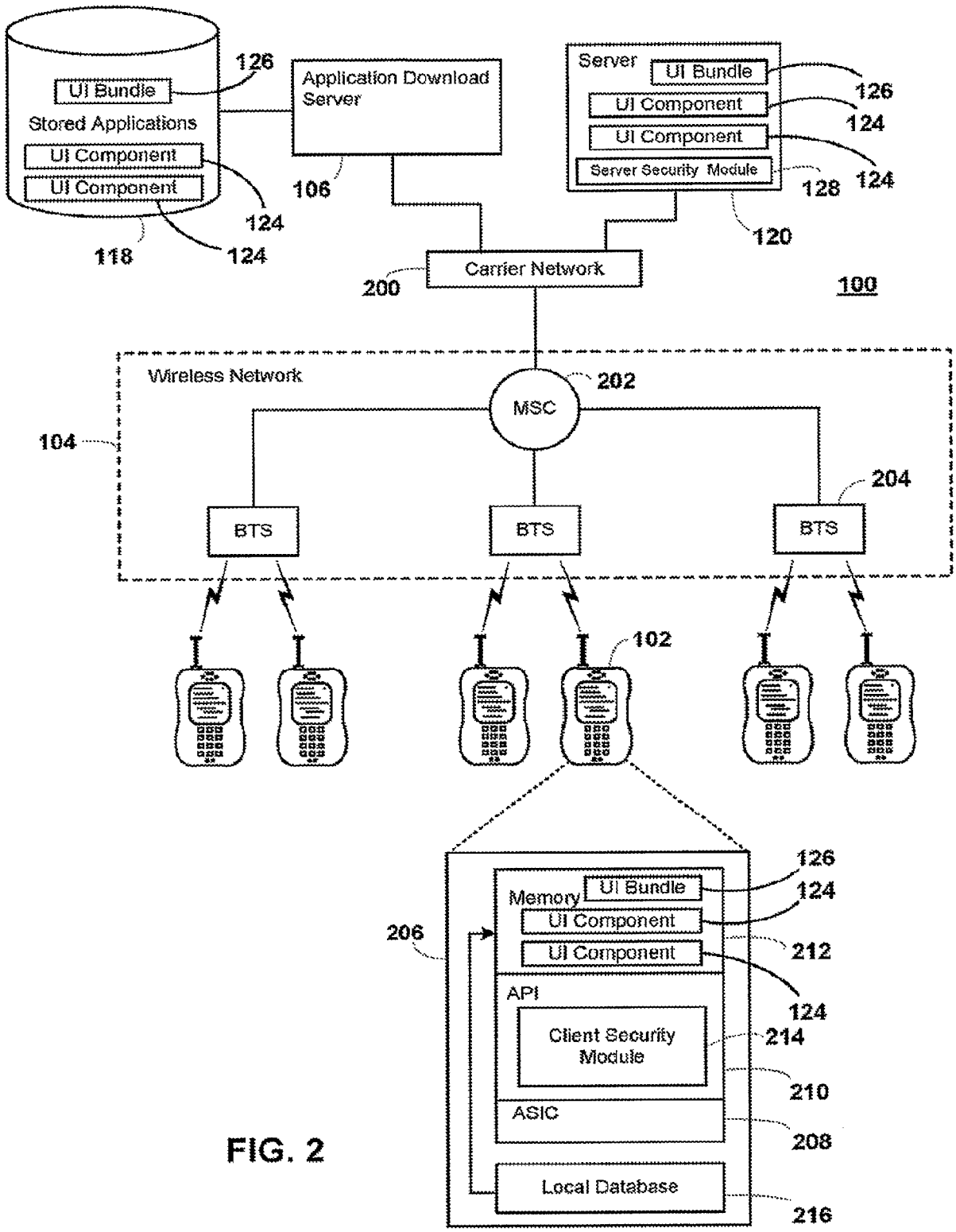

UI Bundle
Stored Applications
UI Component
UI Component
126
124
124
118
Application Download Server
106
Server
UI Bundle
UI Component
UI Component
Server Security Module
126
124
124
128
120
Carrier Network
200
100
Wireless Network
104
MSC
202
BTS
BTS
BTS
204
102
206
Memory
UI Bundle
UI Component
UI Component
126
124
212
API
Client Security Module
124
214
210
ASIC
208
Local Database
216

FIG. 2

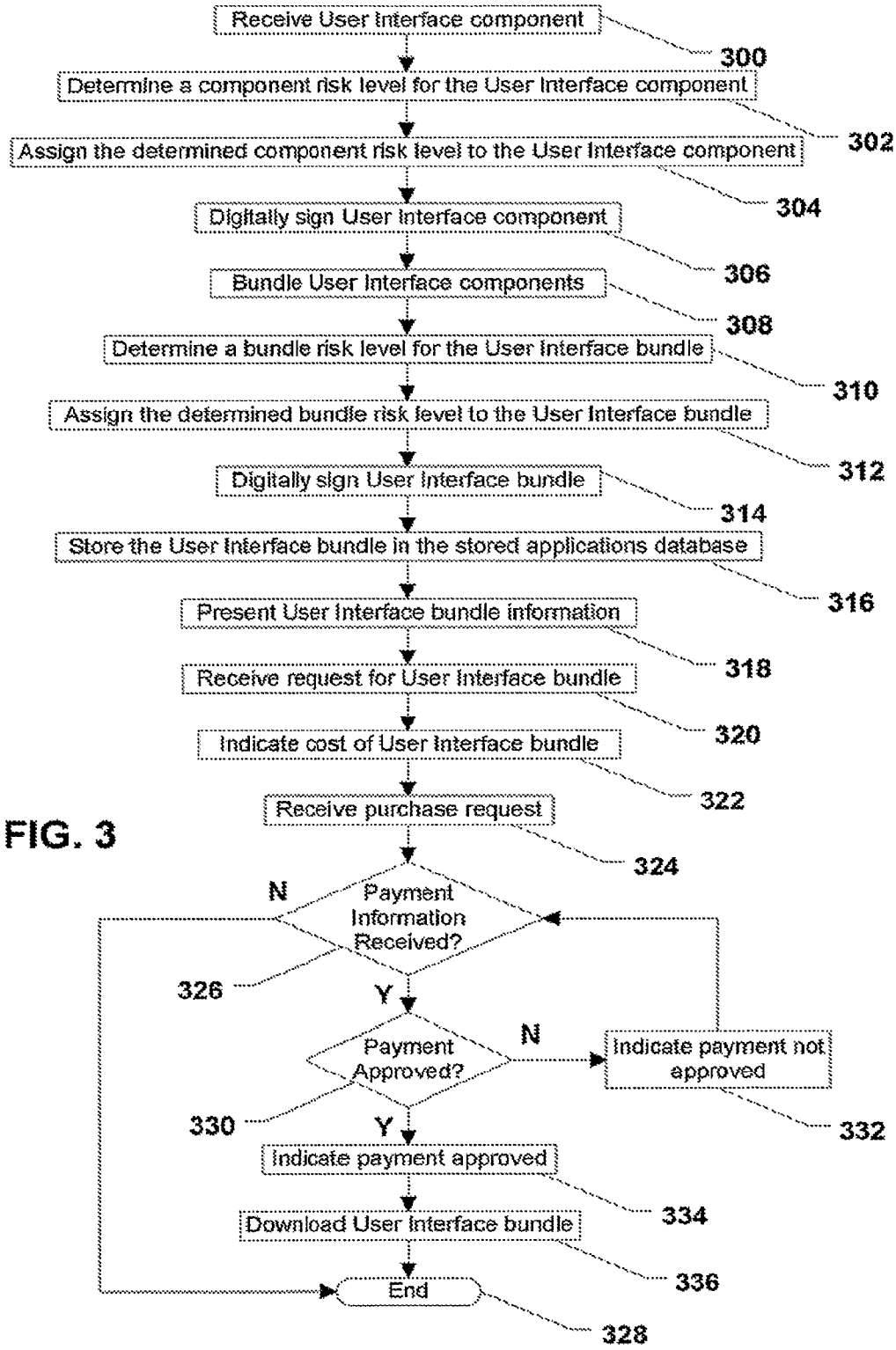

Receive User Interface component
300
Determine a component risk level for the User Interface component
302
Assign the determined component risk level to the User Interface component
304
Digitally sign User Interface component
306
Bundle User Interface components
308
Determine a bundle risk level for the User Interface bundle
310
Assign the determined bundle risk level to the User Interface bundle
312
Digitally sign User Interface bundle
314
Store the User Interface bundle in the stored applications database
316
Present User Interface bundle information
318
Receive request for User Interface bundle
320
Indicate cost of User Interface bundle
322
Receive purchase request
324
Payment Information Received?
N
326
Y
Payment Approved?
N
Indicate payment not approved
332
330
Y
Indicate payment approved
334
Download User Interface bundle
336
End
328

FIG. 3

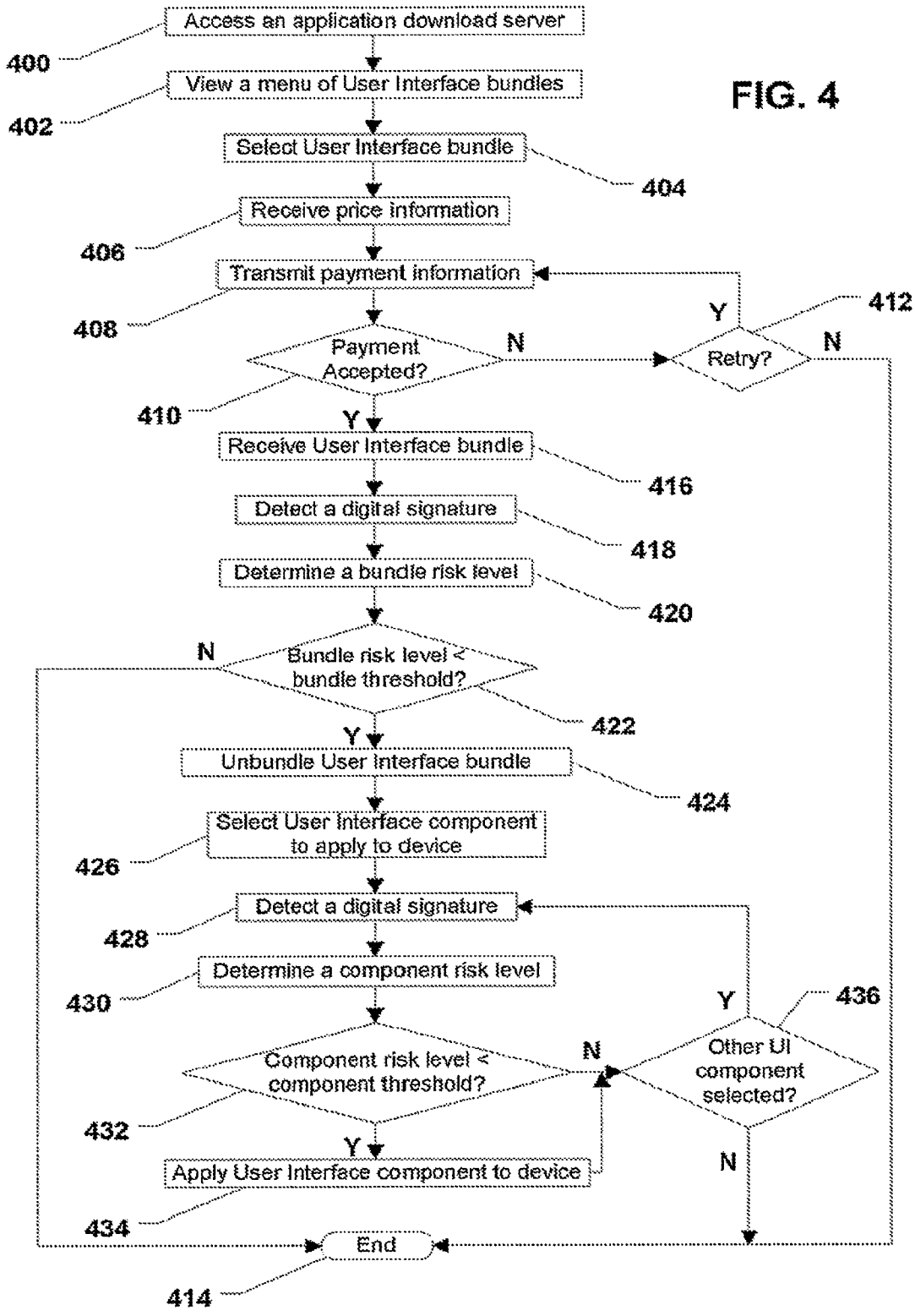

Access an application download server
400
View a menu of User Interface bundles
402
Select User Interface bundle
404
Receive price information
406
Transmit payment information
408
Payment Accepted?
410
N
Y
Retry?
412
Y
N
Receive User Interface bundle
416
Detect a digital signature
418
Determine a bundle risk level
420
Bundle risk level < bundle threshold?
422
N
Y
Unbundle User Interface bundle
424
Select User Interface component to apply to device
426
Detect a digital signature
428
Determine a component risk level
430
Component risk level < component threshold?
432
N
Y
Other UI component selected?
436
Y
N
Apply User Interface component to device
434
End
414

FIG. 4

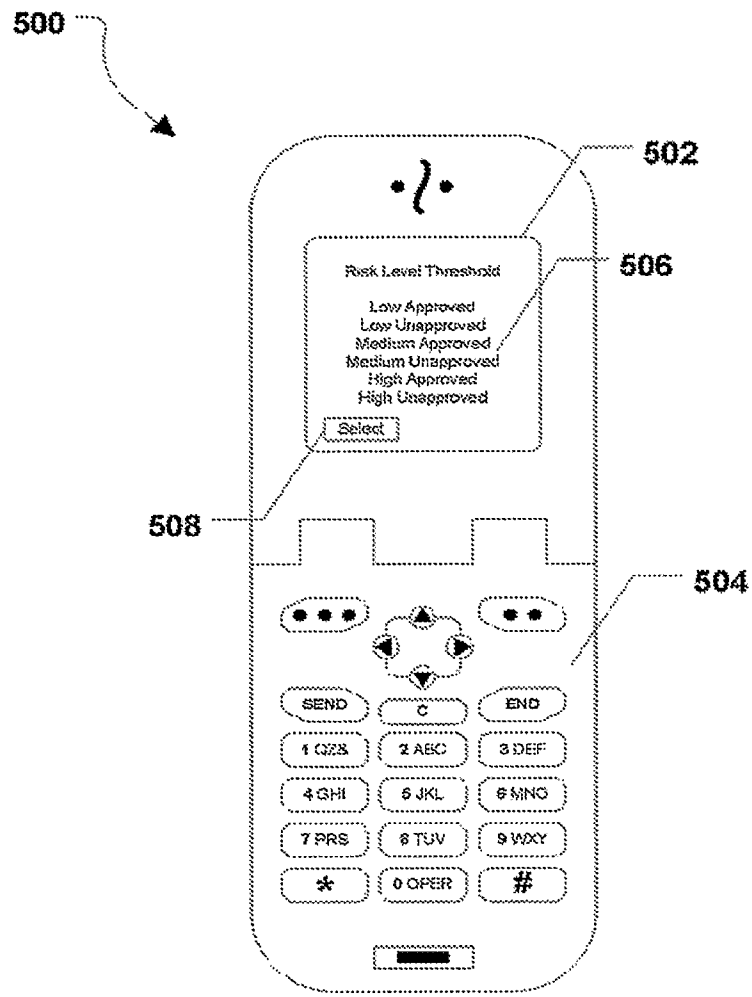

500
502
506
508
504
Risk Level Threshold
Low Approved
Low Unapproved
Medium Approved
Medium Unapproved
High Approved
High Unapproved
Select
SEND
C
END
1 QZ$
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PRS
8 TUV
9 WXY
*
0 OPER
#

FIG. 5

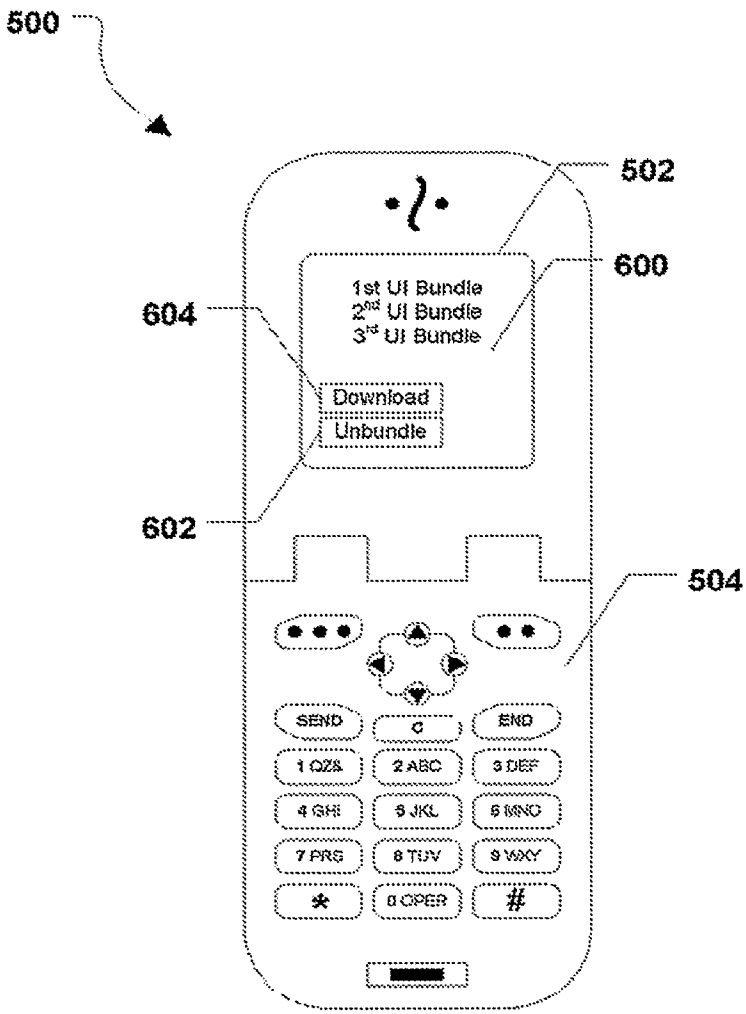

500
502
600
604
602
504
1st UI Bundle
2nd UI Bundle
3rd UI Bundle
Download
Unbundle
SEND
C
END
1 QZ&
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PRS
8 TUV
9 WXY
*
0 OPER
#

FIG. 6

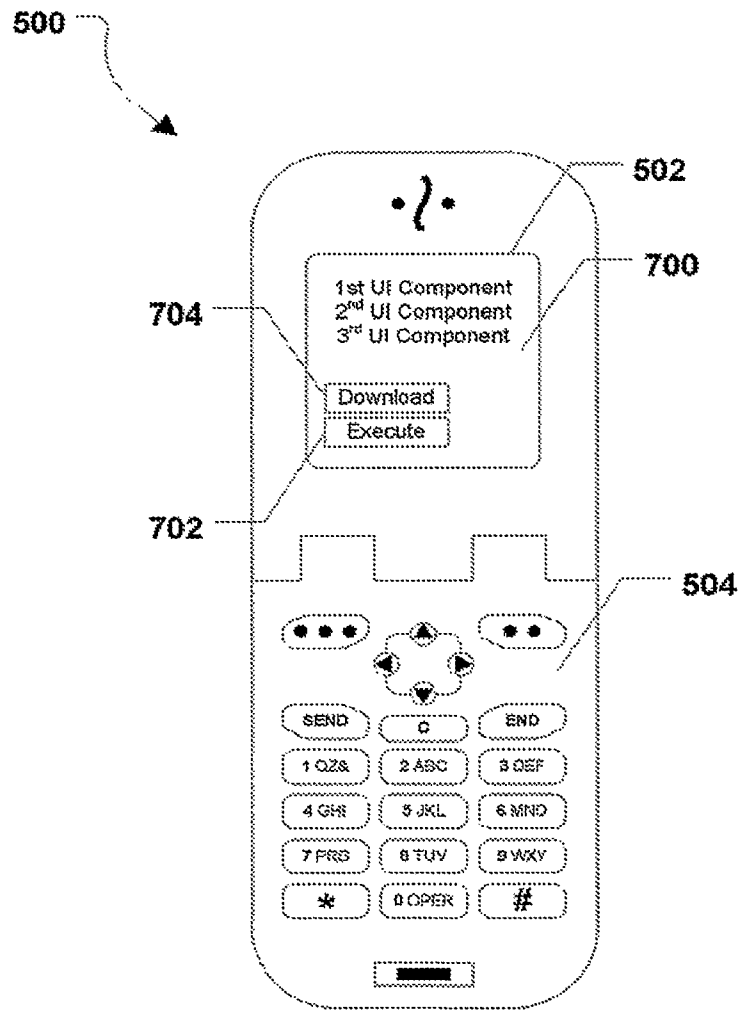

500
502
700
704
1st UI Component
2nd UI Component
3rd UI Component
Download
Execute
702
504
SEND
C
END
1 QZ&
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PRS
8 TUV
9 WXY
*
0 OPER
#

FIG. 7

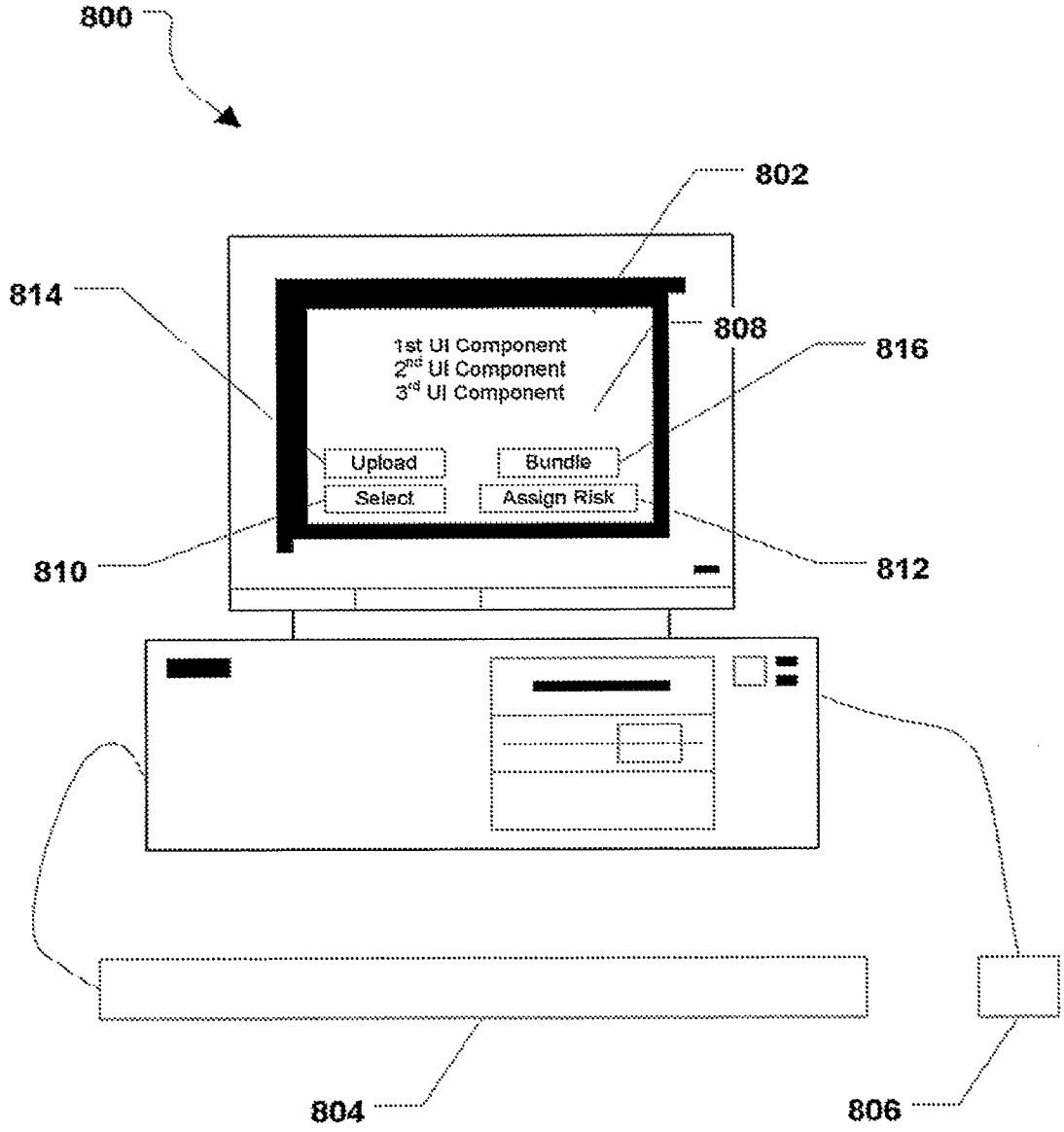

800
802
814
808
816
1st UI Component
2nd UI Component
3rd UI Component
Upload
Bundle
Select
Assign Risk
810
812
804
806

FIG. 8

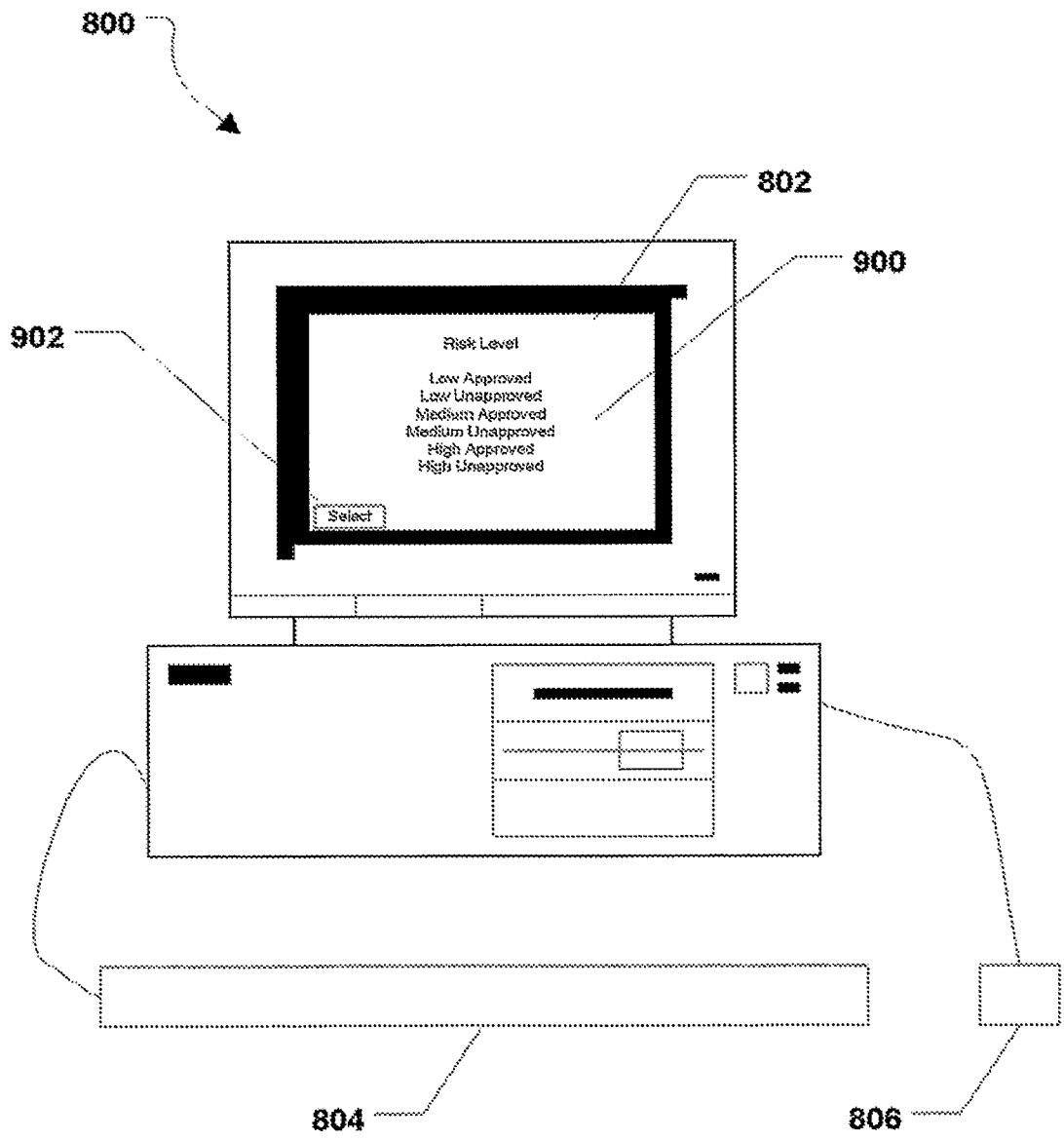

800
802
900
902
Risk Level
Low Approved
Low Unapproved
Medium Approved
Medium Unapproved
High Approved
High Unapproved
Select
804
806

FIG. 9

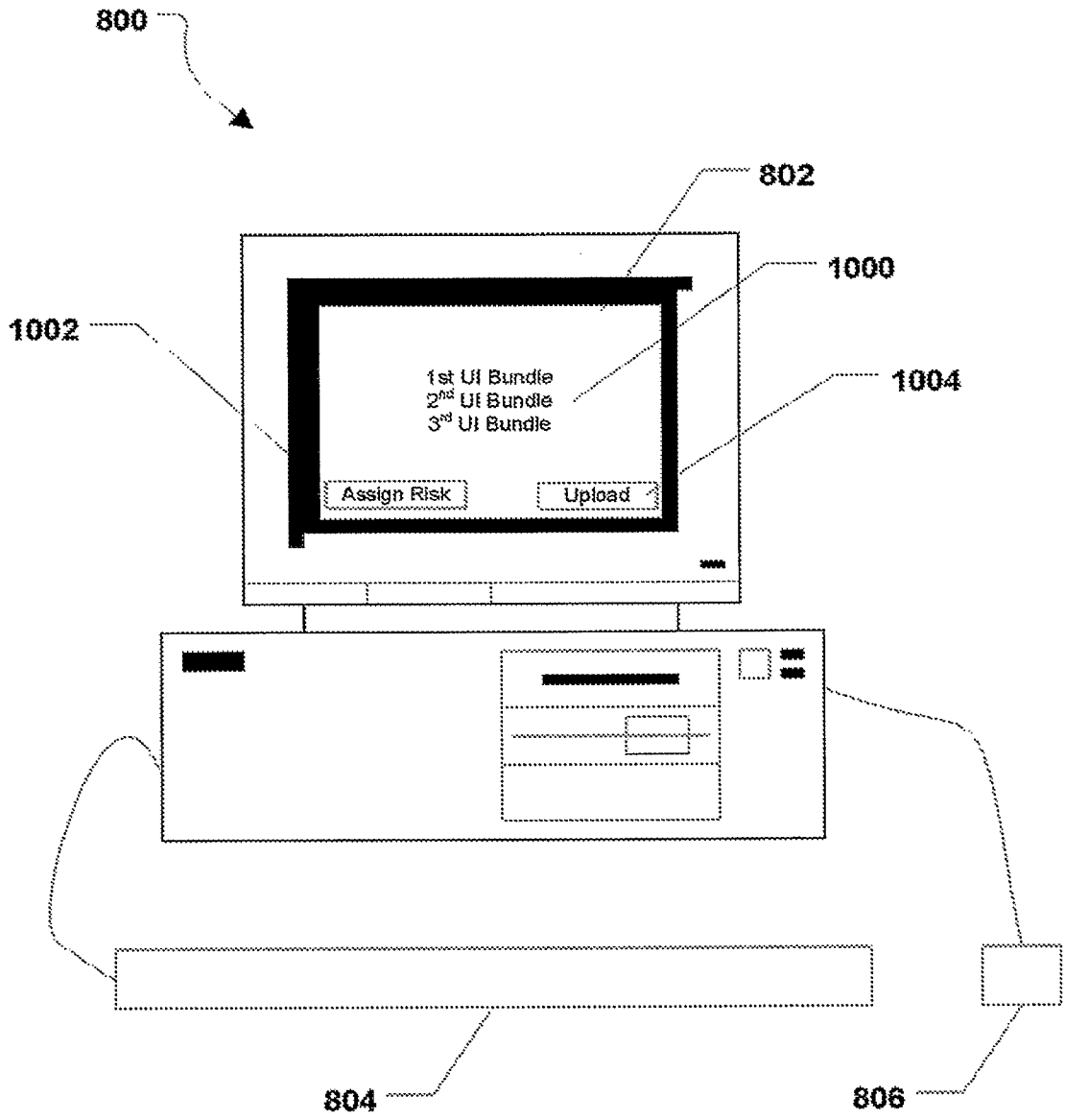

800
802
1000
1002
1004
1st UI Bundle
2nd UI Bundle
3rd UI Bundle
Assign Risk
Upload
804
806

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/062816

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04Q7/32

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04Q G06F H04L

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 practical, 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 03/107201 A (KT FREETEL CO LTD [KR]; KWON JI-HUN [KR]; YIM SEUNG-HYOUK [KR]; NAM GW) 24 December 2003 (2003-12-24) abstract page 1, lines 4-7 page 2, lines 5-17 page 4, line 9 - page 6, line 3 page 7, line 10 - page 9, line 20 page 11, line 13 - page 13, line 20 page 15, line 1 - page 16, line 13 page 17, lines 6-10 page 19, line 5 - page 20, line 11 page 23, lines 5-11 page 24, line 7 - page 25, line 11 page 27, lines 5-17 page 29, lines 7-12 claims 1-20 figures 2-6	1-38

-/--

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

[X] See patent family annex.

* Special categories of cited documents :

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

"E" earlier document 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
14 June 2007	26/06/2007

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Manuel, Grégory

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/062816

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 489 497 A (OPENWAVE SYS INC [US]) 22 December 2004 (2004-12-22) abstract paragraphs [0002], [0006], [0012], [0013], [0019] - [0021], [0030], [0032], [0043], [0044], [0046], [0049] - [0054], [0070], [0077], [0088] - [0092] figures 1-3	1-38
A	US 2003/060189 A1 (MINEAR BRIAN [US] ET AL) 27 March 2003 (2003-03-27) abstract paragraphs [0003], [0004], [0007], [0027], [0031] - [0033], [0037], [0040], [0043], [0045], [0048], [0057], [0061], [0062], [0066], [0070], [0071] paragraphs [0074] - [0081], [0094]	1-38
A	US 2003/149917 A1 (SMITH WILLIAM MARK [US] ET AL) 7 August 2003 (2003-08-07) abstract figures 7,8 paragraphs [0002], [0003], [0017], [0027], [0036] - [0038], [0042] claims 1-36	1-38
A	US 2002/137502 A1 (CRONIN MICHAEL [DE] ET AL CRONIN MICHAEL [DE] ET AL) 26 September 2002 (2002-09-26) abstract paragraphs [0002], [0006] - [0013], [0020], [0023], [0024], [0027], [0037], [0044] - [0046]	1-38
A	US 2005/210448 A1 (KIPMAN ALEX A [US] ET AL) 22 September 2005 (2005-09-22) abstract figures 1-7 paragraphs [0002], [0004], [0006], [0007], [0018], [0023], [0024], [0049], [0068]	1-38
A	NETSCAPE COMMUNICATIONS CORPORATION: "Establishing trust for downloaded software" INTERNET CITATION, [Online] 2 July 1997 (1997-07-02), XP002155043 Retrieved from the Internet: URL:http://developer.netscape.com:80/docs/manuals/signedobj/trust/owp.htm> [retrieved on 2000-12-08] the whole document	1-38

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/062816

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 03107201 A	24-12-2003	AU 2002368021 A1	31-12-2003
		KR 20030085270 A	05-11-2003
EP 1489497 A	22-12-2004	US 2005021935 A1	27-01-2005
US 2003060189 A1	27-03-2003	US 2006281440 A1	14-12-2006
US 2003149917 A1	07-08-2003	DE 10257428 A1	28-08-2003
		GB 2388679 A	19-11-2003
		JP 2004005417 A	08-01-2004
US 2002137502 A1	26-09-2002	DE 20104839 U1	22-08-2002
US 2005210448 A1	22-09-2005	NONE	