

(43) International Publication Date
16 September 2010 (16.09.2010)

PCT

(10) International Publication Number
WO 2010/104511 A1

(51) International Patent Classification:

G06F 15/16 (2006.01) **G06K 17/00** (2006.01)
H04B 5/02 (2006.01) **G06F 21/00** (2006.01)

(21) International Application Number:

PCT/US2009/036918

(22) International Filing Date:

12 March 2009 (12.03.2009)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant (for all designated States except US):
HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. [US/US]; 11445 Compaq Center Drive W., Houston, TX 77070 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **HOCHMUTH, Roland, M.** [US/US]; 3404 E. Harmony Rd., B-6 61 J9, Mail Stop 73-6lj9, Ft. Collins, CO 80528-9544 (US).
KING, James, M. [US/US]; 3404 E. Harmony Rd., B-6 61 G10-641, Mail Stop 73-6ll11, Ft. Collins, CO 80527-9544 (US). **TROUTMAN, Roy, Lee** [US/US]; 3404 E. Harmony Rd., B-6 61 J10, Mail Stop 73-6lj10, Ft. Collins, CO 80527-9544 (US).(74) Agents: **REDDY, Arvind** et al.; Intellectual Property Administration, Mail Stop 35, P.O. Box 272400, Fort Collins, CO 80527-2400 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, 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), European (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, 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 the identity of the inventor (Rule 4.17(i))
- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

Published:

- with international search report (Art. 21(3))

(54) Title: DYNAMIC REMOTE PERIPHERAL BINDING

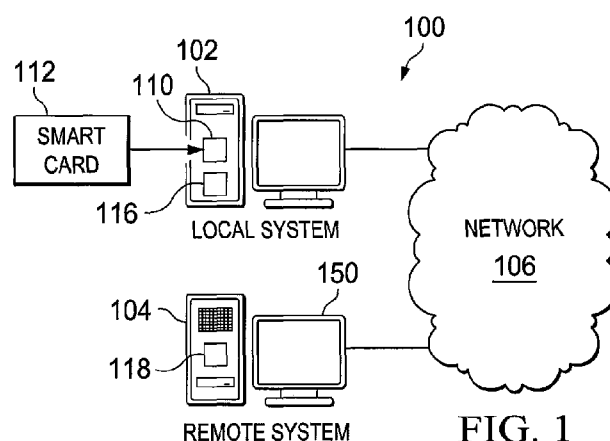


FIG. 1

(57) Abstract: Disclosed are systems and methods of dynamic remote peripheral binding. In one embodiment, such a system includes a local system (102) configured to bind a smart card reader (110) to the local system (102). The smart card reader (110) is configured to extract data from a smart card (112). The system includes a local authentication engine (120) that prompts the user for user authentication information associated with the smart card (112). The local authentication engine (120) authenticates that the user is associated with the smart card (112), is authorized to access the user credentials and extracts them from the smart card (112). A remote access client (116) module establishes a remote session (121) from the local system (102) to a remote system (104). The local system (102) unbinds the smart card reader (110) from the local system (102) and binds the smart card reader (110) to the remote system (104).



WO 2010/104511 A1

DYNAMIC REMOTE PERIPHERAL BINDING

BACKGROUND

[0001] An operating system (commonly abbreviated OS and O/S) is the software component of a computer system that is responsible for the management and coordination of activities and the sharing of the resources of the computer. The operating system acts as a host for application programs that are run on the machine. As a host, one of the purposes of an operating system is to handle the details of the operation of the hardware. This relieves application programs from having to manage these details and makes it easier to write applications. Almost all computers, including hand-held computers, desktop computers, supercomputers, and even modern video game consoles, use an operating system of some type. A thin-client is an example of a desktop computer or local system that may run a version of an operating system that is not as powerful as the standard desktop operating system that is used to connect to other computers. On the local system a remote access client software may be initialized to connect to a remote system.

BRIEF DESCRIPTION

[0002] Many aspects of the disclosure can be better understood with reference to the following drawings. The components in the drawings are not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the present disclosure. Moreover, in the drawings, like reference numerals designate corresponding parts throughout the several views. While several embodiments are described in connection with these drawings, there is no intent

to limit the disclosure to the embodiment or embodiments disclosed herein. On the contrary, the intent is to cover all alternatives, modifications, and equivalents.

[0003] FIG. 1 illustrates a networked environment in accordance with an embodiment of the disclosure.

[0004] FIG. 2 is a block diagram of a local system of FIG. 1 from the networked environment of FIG. 1 in accordance with an embodiment of the disclosure.

[0005] FIG. 3 is a block diagram of a local system of FIG. 1 in communication with a remote system of FIG. 1 in accordance with an embodiment of the disclosure.

[0006] FIG. 4 is a flow diagram of an exemplary embodiment of a method of dynamic remote peripheral binding employing a local system of FIG. 1 and a remote system of FIG. 1.

[0007] FIG. 5 is a flow diagram of an alternative exemplary embodiment of a method of dynamic remote peripheral binding employing a local system of FIG. 1 and a remote system of FIG. 1.

[0008] FIG. 6 is a flow diagram of an alternative exemplary embodiment of a method of dynamic remote peripheral binding employing a local system of FIG. 1 and a remote system of FIG. 1.

[0009] FIG. 7 is a flow diagram of an exemplary embodiment of local system of FIG. 1 and/or remote system of FIG. 1 behavior in response to smart card removal.

DETAILED DESCRIPTION

[0010] Single sign-on (SSO) is a method of access control used by remote systems that enables a user to log in once and gain access to the resources of

multiple software systems or services without being prompted to log in again.

Single sign-off is the reverse process whereby a single action of signing out terminates access to multiple software systems. As different applications and resources support different authentication mechanisms, single sign-on internally translates and stores different credentials compared to what may be used for initial authentication.

[0011] Example embodiments of SSO may implement centralized authentication servers that all other applications and systems utilize for authentication purposes, and may combine this with techniques to ensure that users do not actively have to enter their credentials more than once.

[0012] Enterprise single sign-on (E-SSO) systems may be designed to minimize the number of times that a user types an ID and password to sign into multiple applications. The E-SSO solution automatically logs users in, and acts as a password filler where automatic login is not possible. Each client may be given a token that handles the authentication. In an alternative embodiment of an E-SSO solution, each client has E-SSO software stored on the computer to handle the authentication. On the server side, an E-SSO authentication server may be integrated into the enterprise network.

[0013] In addition, smart card authentication may be employed to provide a hardware level security element in SSO and/or E-SSO systems. In a remote visualization system, a system in which, for example, a local system can access a remote desktop or other remotely-run application which is displayed on the local system, embodiments of the disclosure can employ smart card authentication for access to the local system as well as the remote system. This disclosure also presents systems and methods where peripheral devices such as

a smart card reader can dynamically bind to local systems and/or remote systems.

[0014] In the context of this disclosure, in some embodiments, when a peripheral device binds to a local system and/or remote system, the system to which the peripheral device binds can have exclusive access to the peripheral. In other embodiments, when a peripheral device binds to a local system and/or remote system, the system to which the peripheral binds can have non-exclusive access to the device. It should be appreciated that a peripheral device can bind to a local system via a local connection such as a USB connection, serial connection, or the like. Alternatively, a peripheral can bind to a remote system via a local system that is in communication with the remote system over a network. In some embodiments, both local and remote systems can use peripheral devices for user authentication. For example, smart card readers can be used locally by a local system for user authentication purposes as well as by remote systems for authentication by a remote access server.

[0015] Accordingly, with reference to FIG. 1, shown is one example of a networked environment 100 according to an embodiment of the disclosure. In one embodiment, a local system 102 is configured to communicate with a remote system 104. In the depicted embodiment, the local system 102 is further configured to communicate with a network 106. Likewise, the remote system 104 can be configured to communicate with the network 106, thereby facilitating communication between the local system 102 and remote system 104. The network 106 may include, for example, any type of network environment such as the Internet, intranets, local area networks, wide area networks (WANs), wireless

networks, cellular networks, phone networks, or other suitable networks or combination of networks.

[0016] The depicted local system 102 can include a personal computer, a thin-client computing device, or other computing system as can be appreciated. The remote system 104 can include a personal computer, server, authentication device, or other computing system as can be appreciated. In one embodiment, the local system 102 can include a thin client computing device configured to access computing resources, storage resources, software resources, and other resources housed within or available to the remote system 104. Accordingly, users of the networked environment 100 can access resources of the remote system 104 from various locations, and the remote system 104 can maintain profile information, preferences, and other data regarding the user to allow a user to access software applications housed within or available to the remote system 104. In this way, the remote system 104 can assign a virtual desktop to various users, which can be consistent regardless of the location of the user. In addition, such a system facilitates deployment, maintenance, and replacement of local system(s) 102, as thin client devices can be deployed as local systems 102 with significant computing resources required by users residing on or accessible to the remote system 104. Such architecture can make significant computing resources available to the local systems 102 depending on the needs of a user, while facilitating the use of low cost thin client devices as local systems 102 in the networked environment 100.

[0017] The local system 102 can further include a peripheral device attached thereto via universal serial bus (USB), Ethernet, IEEE-1394, serial, and/or parallel ports or other connection standards as can be appreciated. In one

embodiment, the peripheral device includes a smart card reader 110 configured to access, read, and/or write a smart card 112. Accordingly, in one embodiment, the local system 102 can accept and access a smart card 112 of a user via the smart card reader 110, where the smart card 112 is encoded with various information about the user. Such information can include, but is not limited to: a user credential, authorization token, public key, private key or other authentication or user data as can be appreciated. Data encryption and/or decryption can also be employed to store and/or extract certain data from the smart card 112. In one embodiment, the smart card 112 can include unencrypted data as well as encrypted data. The unencrypted data can include less sensitive data such as a user name, public key, *etc.*, while the encrypted data can include more sensitive data such as a password, user credential, private key, *etc.*

[0018] Accordingly, the smart card reader 110 can bind to the local system 102 and facilitate use of a smart card 112 to authenticate a user to the local system 102. In addition, the smart card reader 110 can bind to the remote system 104 via the local system 102 and the network 106. Therefore, according to an embodiment of the disclosure, a smart card reader 110 accessed by a local system 102 can bind to the remote system 104 to facilitate authentication of the user to the remote system 104. The above functionality is but one example of an embodiment according to the disclosure, as it should be appreciated that any peripheral device can bind to the local system 102 as well as to the remote system 104. Accordingly, the local system 102 and remote system 104 can access any type of peripheral device coupled to the local system 102.

[0019] With reference to FIG. 2, shown is one example of a local system 102 according to an embodiment of the disclosure. FIG. 2 depicts a local system 102 having a memory 124 and a processor 142 configured to execute various software components to facilitate authentication of a user employing a smart card 112 accessed by a smart card reader 110. For example, the memory 124 and processor 142 can communicate with a data bus 125, with which the smart card reader 110 can also communicate. Accordingly, upon insertion of a smart card 112 in the smart card reader 110, a peripheral device event can be generated by the smart card reader 110, which can be handled by a local authentication engine 120, which, in one embodiment, is stored in memory 124 and executable by the processor 142. The local system 102 executes the local authentication engine 120 to extract various user data from a smart card 112 in order to authenticate and/or identify a user to which the smart card 112 belongs and/or is assigned.

[0020] In one embodiment, the local authentication engine 120 of the local system 102, upon entry of a smart card 112 in the smart card reader 110, can authenticate the user and provide access to the local system 102. In other words, the local authentication engine 120 can grant access to the local system 102 for a user if the user possesses a smart card having proper user credentials stored thereon. In another embodiment, the local authentication engine 120 can prompt a user for additional authentication information such as a password, personal identification number, or other user provided authentication information. In other words, the local authentication engine 120 can provide an additional layer of security by prompting a user for user supplied credentials that can be verified using the data stored on the smart card 112. To facilitate the above, the

smart card reader 110 binds to the local system 102 in that it is available, either exclusively or non-exclusively, to the local authentication engine 120 of the local system 102.

[0021] The local system 102 can further execute a remote access client 116 in order to facilitate communication between the local system 102 and a remote system 104. Accordingly, reference is now made to FIG. 3, which depicts a local system 102 in communication with a remote system 104. In order to facilitate communication between the local system 102 and remote system 104, the local system 102 can execute a remote access client 116. Likewise, the remote system 104 can execute a remote access server 132 configured to communicate with the remote access client 116 to facilitate such functionality. The local system 102 and/or remote system 104 can establish a remote session 121 for a user wishing to gain access to the remote system 104 via the local system 102. The remote session 121 can include various user profile information, preferences, and other data facilitating virtual desktop and/or remote access functionality for various users as noted above in reference to FIG. 1.

[0022] In one embodiment, upon insertion of a smart card 112 in the smart card reader 110 of the local system 102, the smart card reader 110 can trigger an event that can be handled by the remote access client 116. Accordingly, the remote access client 116 can establish a remote peripheral session 128 corresponding to a remote session 121 established for a user, which allows the remote access client 116 to extract and/or access information from the smart card 112 via the smart card reader 110 as noted above. The remote access client 116 can communicate data regarding the smart card 112 and smart card reader 110 within the remote peripheral session 128 and remote session 121 to

the remote access server 132 stored in a memory 130 and executed by a processor 143.

[0023] The remote access server 132 can accordingly establish a server based remote peripheral session 133 in the remote system 104. In one embodiment, the server based remote peripheral session 133 can give the remote system 104 exclusive access to the smart card 112 and smart card reader 110, thereby unbinding the smart card reader 110 from the local system 102 and binding the smart card reader 110 to the remote system 104. Upon binding of the smart card reader 110 to the remote system 104, a remote authentication engine 134 can extract data regarding a user encoded on the smart card 112 in order to authenticate the user. In one embodiment, a user can present a smart card 112 to the local system 102, which can establish a remote session 121 having a remote peripheral session 128 to facilitate a physical security layer that can be imposed on top of a software password authentication scheme.

[0024] Accordingly, a server based remote peripheral session 133 can give exclusive access to the smart card reader 110 to the remote system 104, and the remote authentication engine 134 can authenticate a user's credentials, which may be stored on and extracted from the smart card 112. The remote authentication engine 134 can also prompt a user for additional authentication information via the remote session 121 and local system 102. As a non-limiting example, the remote authentication engine 134 can request a personal identification number, password, and/or other authentication data from a user, which can be received by the local system 102 via an input device and transmitted to the remote system 104 via the network 106. A user may terminate the remote session 121 and/or connectivity to the remote system 104, which

subsequently unbinds the smart card reader 110 from the remote system 104.

Accordingly, the smart card 112 and smart card reader 110 can again bind to the local system 102 upon termination of a remote session 121.

[0025] In another embodiment, the local system 102 can locally authenticate a user via the local authentication engine 120 prior to establishing a remote session 121 and/or communication with the remote system 104. Upon establishing a remote session 121, the smart card reader 110 can unbind from the local system 102 and bind to the remote system 104. Accordingly, the remote system 104 can then extract data from and/or access the smart card 112 and smart card reader 110.

[0026] Reference is now made to FIG. 4, which depicts one example of a process according to one embodiment of the disclosure. The flowchart of FIG. 2 can also be viewed as a method of remote peripheral binding. In block 205, a user can initiate a remote access client 116 (FIG. 3) in a local system 102 (FIG. 1). In block 210, the user slides, inserts, or otherwise provides access to a smart card 112 (FIG. 1) to a smart card reader 110 (FIG. 1). In block 215, the smart card reader 110 is attached as a local peripheral device of the local system 102. In block 220, the local authentication engine 120 (FIG. 3) receives notification of the smart card event and communicates with the locally attached peripheral device to extract user credentials from the smart card 112. In block 225, the remote access client 116 (FIG. 3) facilitates determination of a remote access server 132 (FIG. 3) that the user may connect to based on the user credentials returned by the smart card 112, an internet protocol address entered by the user, or other data as can be appreciated.

[0027] In block 235, the remote access client 116 establishes a connection to the remote access server. The connection may be an anonymous connection. In block 240, the remote access client 116 unbinds the smart card reader 110 from the local system 102. At this time the smart card reader is no longer available for use by software on the local system 102 other than the remote access client 116. For example, the local authentication engine 120 can no longer access the smart card reader 110. In block 245, the remote access client 116 binds the locally attached smart card reader to the remote access server 132.

[0028] In block 250, the remote access server 132 establishes a server based remote peripheral session 133 (FIG. 3) based upon a remote session 121 created for a user. The smart card reader 110 is now available to the remote access server 132 and a remote authentication engine 134 (FIG. 3). The user may then authenticate himself to the remote access server 132. If the remote access server 132 is configured to use smart card authentication, the smart card can be accessed using the server based remote peripheral session 133.

[0029] When the remote session 121 is terminated, the smart card reader 110 is unbound from the remote system 104 and bound to the local system 102. Accordingly, the smart card reader 110 can be available for subsequent reconnects to the remote system 104. Accordingly, the smart card reader 110 is available for use by the local system 102, as the remote system 104 has released its use thereof. Although the above method discusses the use of smart cards as examples, it should be appreciated that the systems and methods disclosed herein can apply to any peripheral device to which a local system 102 and a remote system 104 may require access and/or exclusive access.

[0030] Referring to FIG. 5, flow diagram 300 provides one example of an embodiment of a method for remote peripheral binding in accordance with the disclosure. In block 310, the local system 102 (FIG. 1) receives a smart card 112 (FIG. 1) in a smart card reader 110 (FIG. 1). In the absence of a remote session 121 established by a remote access client 116 (FIG. 1) in the local system 102, the smart card reader 110 is bound to the local system 102. In block 330, the user can be prompted for a personal identification number (PIN) or other authentication information. A user may enter such authentication information in the local system 102 via an input device such as a keyboard, mouse, etc. In block 340, the local system 102 receives the PIN and a remote session 121 (FIG. 3) is established. In block 350, the smart card reader is unbound from the local system after a connection is established between a remote access client 116 (FIG. 3) in the local system 102 and a remote access server 132 (FIG. 3) in the remote system 104 (FIG. 1). In block 360, the smart card reader is unbound from the local system 102 and bound to the remote system 104 via the remote access client 116 and remote access server 132, which facilitate creation of a server based remote peripheral session 133 in the remote system 104.

[0031] Example embodiments of methods of dynamic peripheral binding, as disclosed herein, allow non-limiting exemplary smart card readers 110 (FIG. 1) to be dynamically bound to the local system 102 (FIG. 1) and the remote system 104 (FIG. 1) after a connection is established between the local system 102 and remote system 104. This allows peripheral devices such as a smart card reader 110 to be used both locally and remotely. Referring now to an alternative exemplary embodiment of remote peripheral binding in FIG. 6, a user can access a local system 102 and request further access to a remote system 104 via the

local system 102 by inserting a smart card 112 (FIG. .1) in a smart card reader 110 bound to the local system 102. In block 410, the local system 102 receives the smart card.

[0032] In block 430, the local system 102 extracts user credentials from the smart card 112. In one embodiment, a username can be extracted from the smart card 112 from an unencrypted portion of the smart card 112 data. In another embodiment, the local system 102 can extract and decrypt user credential data from the smart card 112. In block 440, the remote access client 116 (FIG. 3) queries a database to determine a remote system 104 (FIG. 3) with which to connect. Upon determination of a remote system 104 to which to connect, the local system 102 can display a user interface corresponding to an authentication screen, virtual desktop, user profile data, user preferences, or other data as can be appreciated from the remote system 104.

[0033] Accordingly, the remote access client 116 can create a remote session 121 (FIG. 3) as well as a remote peripheral session 128, which unbinds the smart card reader 110 from the local system 102 and binds the smart card reader 110 to a server based remote peripheral session 133 (FIG. 3) in a remote access server 132 (FIG. 1). Accordingly, the remote authentication engine 134 (FIG. 3) can extract user credential information from the smart card 112. The remote authentication engine 134 can then cause the remote access client 116 to generate one or more user interface elements requesting authentication information (e.g. a PIN, password, pass-phrase, *etc.*) from a user based upon user credential information extracted from the smart card 112. In block 450, the user can enter authentication information such as a PIN, which is received by the local system 102. In block 460, the remote authentication engine 134 can

determine whether the received PIN is consistent with user credential information extracted from the smart card 112 for verification purposes.

[0034] In block 470, the remote authentication engine 134 accesses the smart card reader 110 and, using the entered PIN, unlocks the smart card 112 to access and/or extract a security certificate stored the smart card 112. In one embodiment, the unlocking may be performed cryptographically based upon the entered PIN, or other data as can be appreciated. In block 480, the the local system 102 can authenticate the user with the extracted security certificate. In one embodiment, the local authentication engine can authenticate the user by querying an Active Directory Domain Controller, for example. In another embodiment, the local authentication engine can transmit the security certificate to the remote system 104, which can employ the remote authentication engine for user authentication.

[0035] In block 490, the smart card reader 110 is unbound from the remote system 104 upon authentication of a user as noted above, as the remote system 104 can terminate the server based remote peripheral session 133, and the remote access client can terminate the remote peripheral session 128, thereby releasing the smart card reader 110 from exclusive use. In block 495, the smart card reader 110 binds to the local system 102 system upon release by the remote access client 116 and remote access server 132. The user is then authenticated to access the local system 102 as well as computing resources of the remote system 104.

[0036] Referring now to FIG. 7, shown is one example of a method in accordance with an embodiment of the disclosure. The method 500 illustrates behavior of the local system 102 and remote system 104 upon removal of a smart card 112

from a smart card reader 110. In one embodiment, to terminate and/or suspend a remote session 121, a user may simply remove a smart card 112 from a smart card reader 110. Upon sensing smart card removal in block 510, the local system 102 can be figured to do one of the following, as non-limiting examples: 1) lock the desktop of the local system 102 in block 520; 2) log the user out from the desktop in block 530; and 3) do nothing. In block 520, a remote session 121 corresponding to a user can be maintained in the local system 102 and/or remote system 104, but the local system 102 and/or remote system 104 can require authentication to allow a user to resume the remote session 121. In block 530, a remote session 121 corresponding to a user can be terminated by the local system 102 and/or remote system 104. If the remote session 121 is terminated, then a user must establish a new remote session 121 as described above.

[0037] If the system has been configured to lock the desktop of a local system 102 in response to removal of a smart card 112 in block 520, then a user may use the same local system 102 or access a different local system 102 and insert his smart card. A user must then reauthenticate in block 540. Accordingly, the the local system 102 can unlock the desktop and the suspended remote session 121 resumed. Such functionality allows a user to lock a desktop on a local system 102, roam to another local system 102, present a smart card 112 and/or other authentication information, and resume the same remote session 121.

[0038] If the system has been configured to log out of the local system 102 in block 530 and terminate the remote session 121, the user can use the same local system 102 or a different local system 102, and present his smart card 112 and/or other authentication information. The same process as previously

described may be followed. The user must be reauthenticated and a new remote session 121 generated.

[0039] If the system has been configured to do nothing in response to removal of a smart card 112, the user can go to a different local system 102 and present his smart card 112 and/or other authentication information. However, on a different local system 102, in block 540, the user must establish a new remote session 121 and authenticate himself to the local system 102 and/or remote system 104.

[0040] The systems and methods of dynamic remote peripheral binding at connect/disconnect disclosed herein allow peripheral devices such as a smart card reader 110 (FIG. 1) and other plug and play devices to be dynamically bound from a local system 102 to a remote system 104 after a remote session 121 (FIG. 1) is established by a user. This allows peripheral devices to be used both locally and then remotely if desired.

[0041] The embodiments disclosed herein can be implemented in hardware, software, firmware, or a combination thereof. At least one embodiment disclosed herein may be implemented in software and/or firmware that is stored in a memory and that is executed by a suitable instruction execution system. If implemented in hardware, one or more of the embodiments disclosed herein can be implemented with any or a combination of the following technologies: a discrete logic circuit(s) having logic gates for implementing logic functions upon data signals, an application specific integrated circuit (ASIC) having appropriate combinational logic gates, a programmable gate array(s) (PGA), a field programmable gate array (FPGA), *etc.*

[0042] The peripheral device logic may reside in memory as instructions which, when executed by a processor means, implement dynamic remote peripheral

binding at connect/disconnect. The processor means may be, for example, a microprocessor, a microcontroller, a network processor, a digital signal processor, a reconfigurable processor, or an extensible processor as non-limiting examples.

[0043] The peripheral device logic may alternatively be implemented in hardware, including, but not limited to, a programmable logic device (PLD), programmable gate array (PGA), field programmable gate array (FPGA), an application-specific integrated circuit (ASIC), a system on chip (SoC), and a system in package (SiP). Furthermore, the peripheral device logic may be implemented as a combination of processor-executable software and hardware logic.

[0044] The flowcharts included herein show the architecture, functionality, and operation of a possible implementation of software. In this regard, each block can be interpreted to represent a software module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that in some alternative implementations, the functions noted in the blocks may occur out of the order and/or not at all. For example, two blocks shown in succession may in fact be executed substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved.

[0045] Any of the programs listed herein, which can include an ordered listing of executable instructions for implementing logical functions, can be embodied in any computer-readable medium for use by or in connection with an instruction execution system, apparatus, or device, such as a computer-based system, processor-containing system, or other system that can fetch the instructions from the instruction execution system, apparatus, or device and execute the

instructions. In the context of this document, a “computer-readable medium” can be any means that can contain or store the program for use by or in connection with the instruction execution system, apparatus, or device. The computer readable medium can be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor storage system, apparatus, or device. More specific examples (a nonexhaustive list) of the computer-readable medium could include a portable computer diskette (magnetic), a random access memory (RAM) (electronic), a read-only memory (ROM) (electronic), an erasable programmable read-only memory (EPROM or Flash memory) (electronic), a portable compact disc read-only memory (CDROM) (optical), a digital versatile disc read-only memory (DVD-ROM) and other storage media as can be appreciated. In addition, the scope of the certain embodiments of this disclosure can include embodying the functionality described in logic embodied in hardware or software-configured mediums.

[0046] One should also note that conditional language, such as, among others, “can,” “could,” “might,” or “may,” unless specifically stated otherwise, or otherwise understood within the context as used, is generally intended to convey that certain embodiments include, while other embodiments do not include, certain features, elements and/or steps. Thus, such conditional language is not generally intended to imply that features, elements and/or steps are in any way required for one or more particular embodiments or that one or more particular embodiments necessarily include logic for deciding, with or without user input or prompting, whether these features, elements and/or steps are included or are to be performed in any particular embodiment.

[0047] It should be emphasized that the above-described embodiments are merely possible examples of implementations, merely set forth for a clear understanding of the principles of this disclosure. Many variations and modifications may be made to the above-described embodiment(s) without departing substantially from the spirit and principles of the disclosure. All such modifications and variations are intended to be included herein within the scope of this disclosure.

CLAIMS

Therefore, at least the following is claimed:

1. A method comprising:

binding a smart card reader (110) to a local system (102), the smart card reader (110) configured to extract data from a smart card (112);

prompting a user for user authentication information (310) associated with the smart card (112), the smart card (112) having user credentials stored thereon;

receiving a user supplied authentication data (340, 430);

authenticating that the user is associated with the smart card (112) and authorized to access the user credentials (460);

extracting the user credentials from the smart card (470);

unbinding the smart card reader from the local system (350);

establishing a remote session (121) from the local system (102) to a remote system (104); and

binding the smart card reader (110) to the remote system (104).

2. The method of claim 1, further comprising the step of employing the extracted user credentials (470) to authenticate the user (480) to the remote system (104).

3. The method of claim 1, wherein the step of authenticating that the user is associated with the smart card (112) and authorized to access the user credentials (460) further comprises extracting a user name from an unencrypted portion of the smart card (430), querying a database for queried authentication data (440) associated with the user name, and authenticating the user supplied authentication data against the queried authentication data (460).

4. The method of claim 3, wherein the user credentials are stored in an encrypted portion (470) of the smart card (112).

5. The method of claim 4, wherein the user credentials are at least one of: a security certificate, a private key, password, and pass phrase (470).

6. The method of claim 1, further comprising the step of determining a remote system (104) with which to establish a remote session (121) from a plurality of remote systems (225).

7. The method of claim 1, further comprising the steps of:
detecting a removal of the smart card (112, 510); and
employing a security measure, the security measure including at least one of: suspending the remote session (520) and terminating the remote session (530).

8. The method of claim 7, further comprising the steps of:
detecting insertion of the smart card (112) in a smart card reader (110); and
prompting the user to reauthenticate that the user is associated with the smart card and authorized to access the user credentials (540).
9. A computer readable storage medium comprising a program for authenticating a user, the program when executed by a computer processor causing the processor to perform the steps of:
binding a smart card reader (110) to a local system (102), the smart card reader (110) configured to extract data from a smart card (112);
prompting a user for user authentication information (310) associated with the smart card (112), the smart card (112) having user credentials stored thereon;
receiving a user supplied authentication data (340, 430);
authenticating that the user is associated with the smart card (112) and authorized to access the user credentials (460);
extracting the user credentials from the smart card (470);
unbinding the smart card reader from the local system (350);
establishing a remote session (121) from the local system (102) to a remote system (104); and
binding the smart card reader (110) to the remote system (104).

10. A system for authenticating a user, comprising:

a local system (102) configured to bind a smart card reader (110) to the local system (102), the smart card reader (110) configured to extract data from a smart card (112);

a local authentication engine (120) configured to prompt the user of the local system (102) for user authentication information associated with the smart card (112), the smart card (112) having user credentials stored thereon and receive a user supplied authentication data, the local authentication engine further configured to authenticate that the user is associated with the smart card (112) and authorized to access the user credentials and extract the user credentials from the smart card (112);

a remote access client (116) module configured to establish a remote session (121) from the local system (102) to a remote system (104); and

wherein the local system (102) unbinds the smart card reader (110) from the local system (102) and binds the smart card reader (110) to the remote system (104).

11. The system of claim 10, wherein the remote system (104) further comprises a remote authentication (134) module configured to receive the extracted user credentials and employ the extracted user credentials to authenticate the user to the remote system (104).

12. The system of claim 10, wherein the local authentication engine (120) is further configured to extract a user name from an unencrypted portion of the smart card (112), query a database for queried authentication data associated with the user name, and authenticate the user supplied authentication data against the queried authentication data.

13. The system of claim 10, wherein the local system (102) is further configured to:

detect a removal of the smart card (112); and

employ a security measure, the security measure including at least one of: suspending the remote session (520) and terminating the remote session (530).

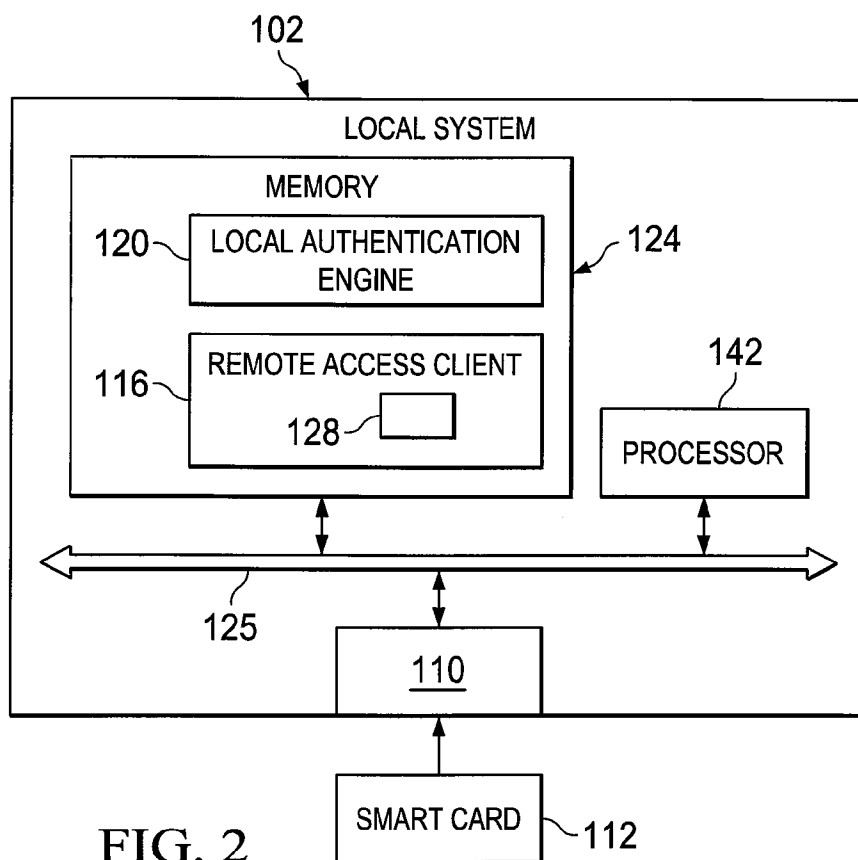
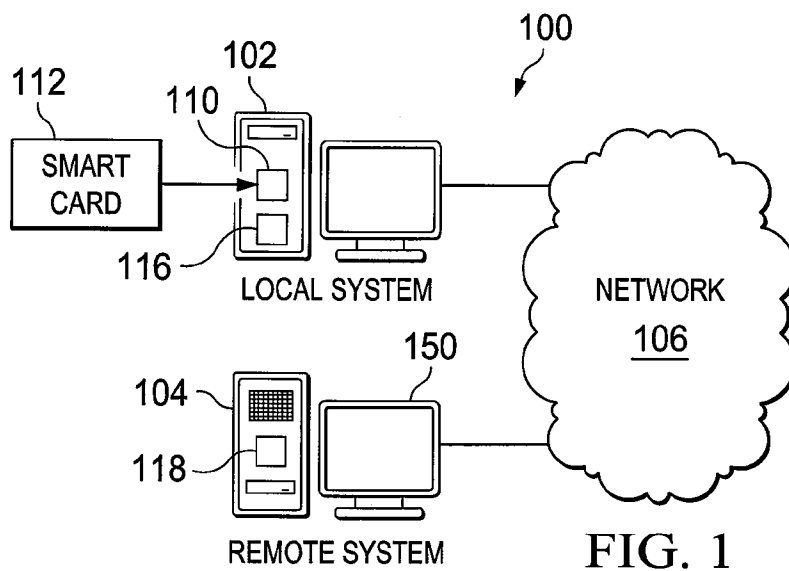
14. The system of claim 13, wherein the local system is further configured to:

detect insertion of the smart card (112) in a smart card reader (110); and

prompt the user to reauthenticate that the user is associated with the smart card (112) and authorized to access the user credentials (540).

15. The system of claim 10, wherein the remote access client (116) determines a remote system (104) with which to establish a remote session (121) from a plurality of remote systems (225).

1/4



2/4

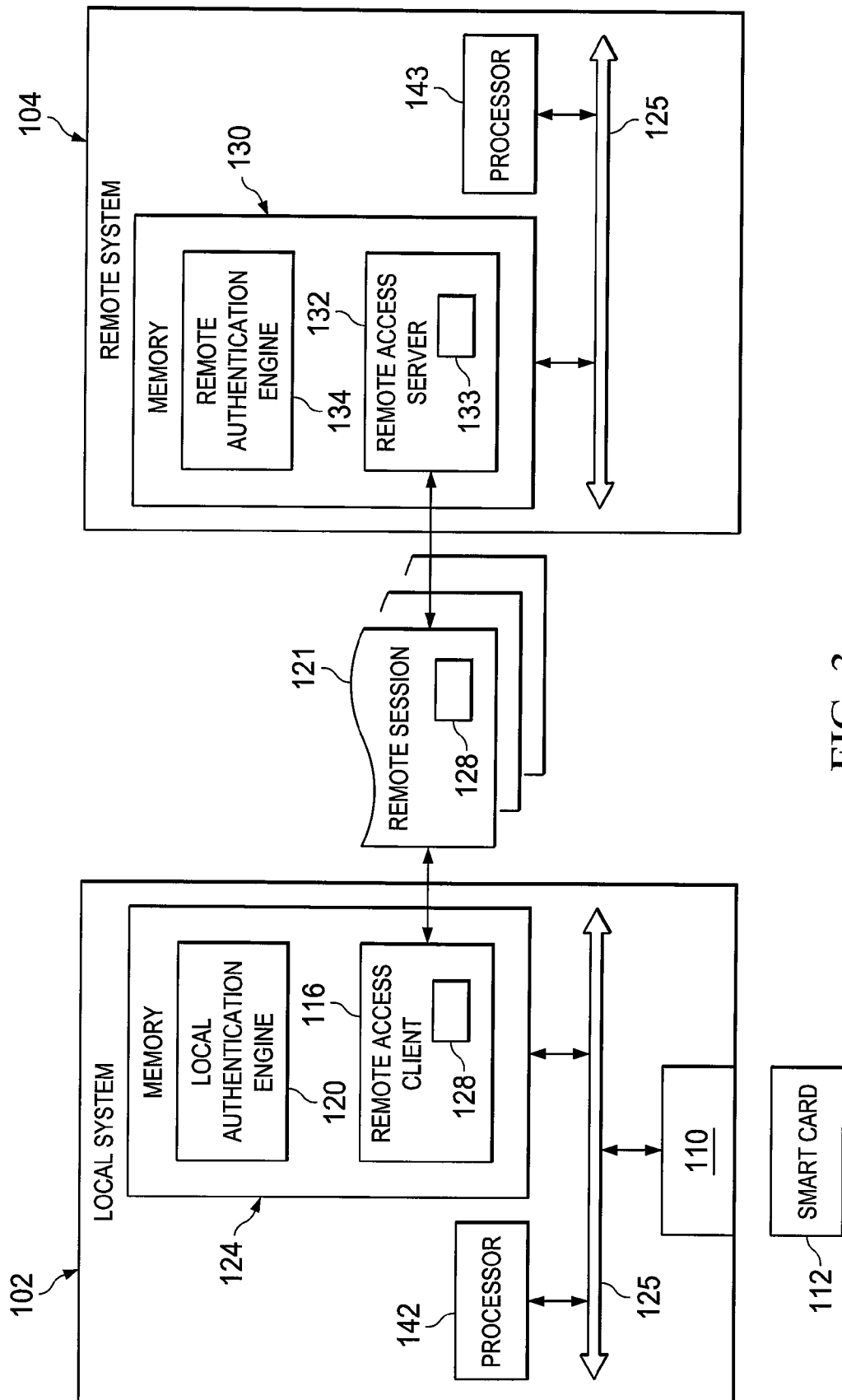


FIG. 3

3/4

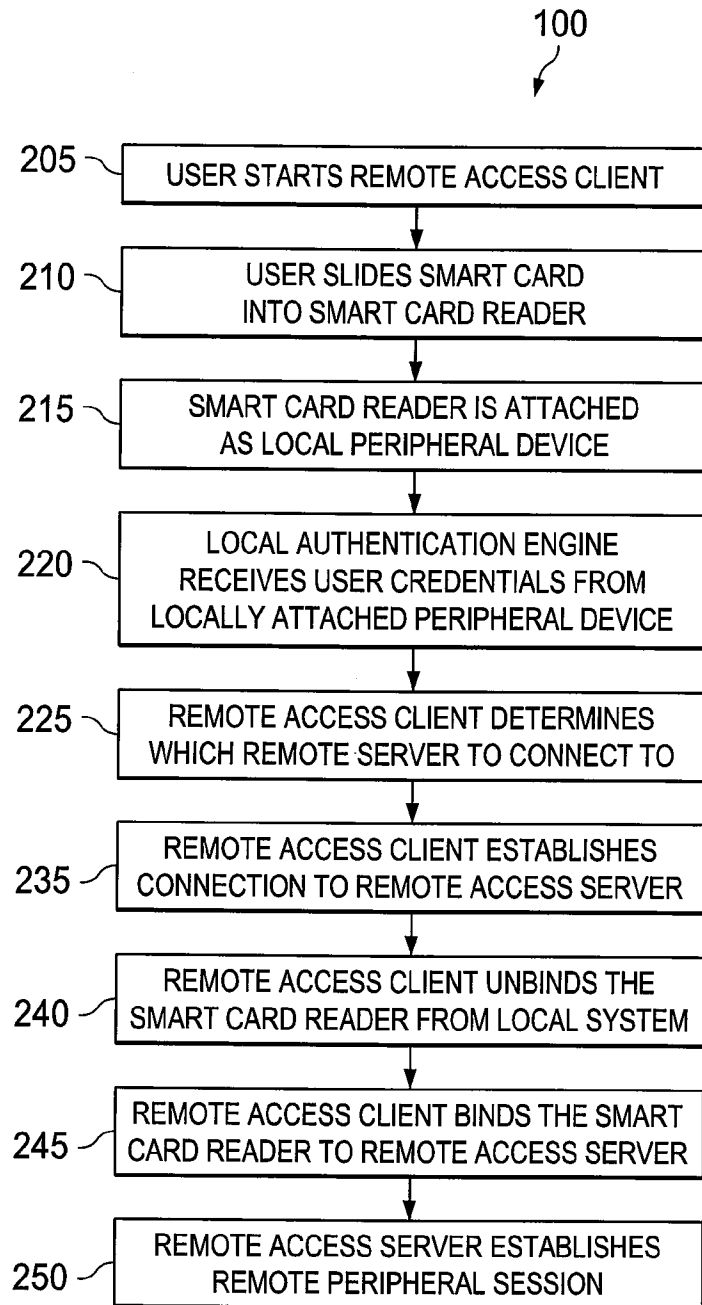


FIG. 4

4/4

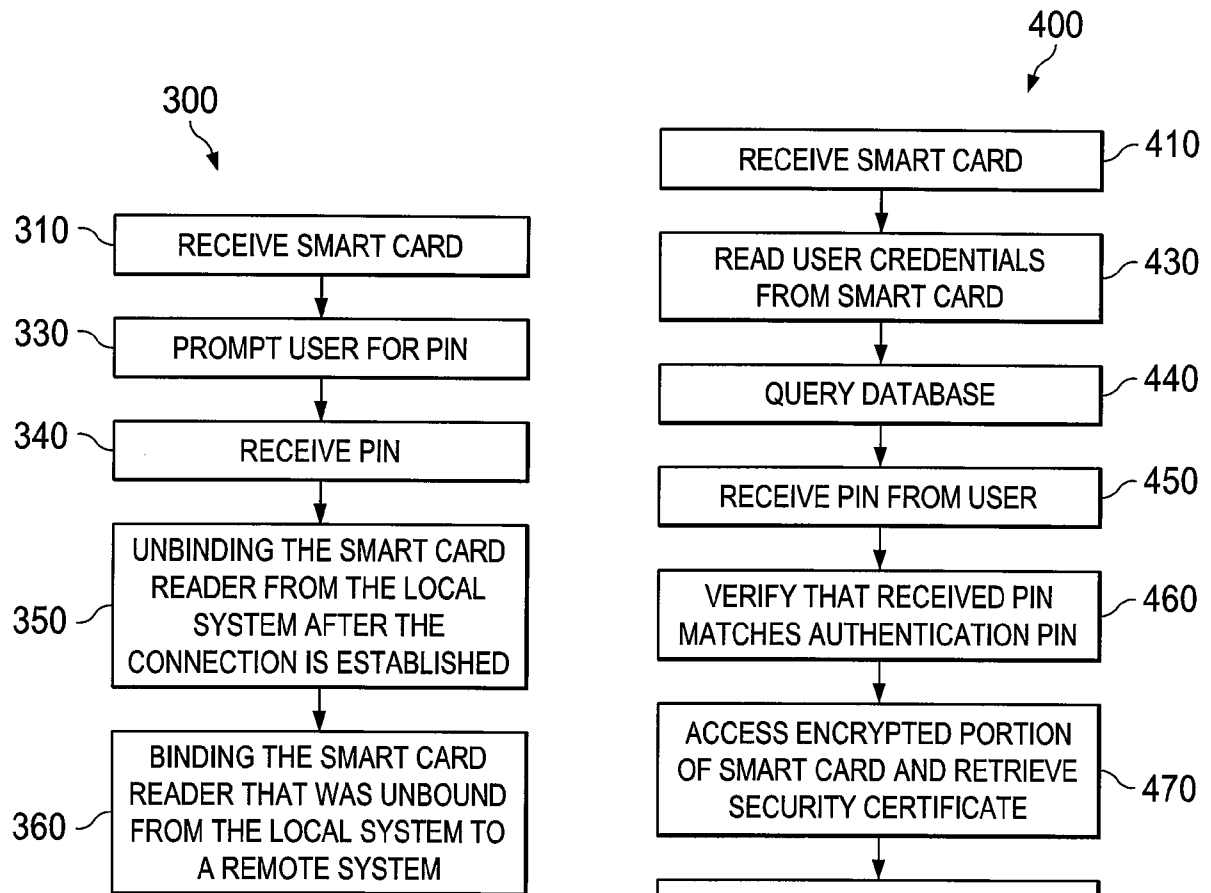


FIG. 5

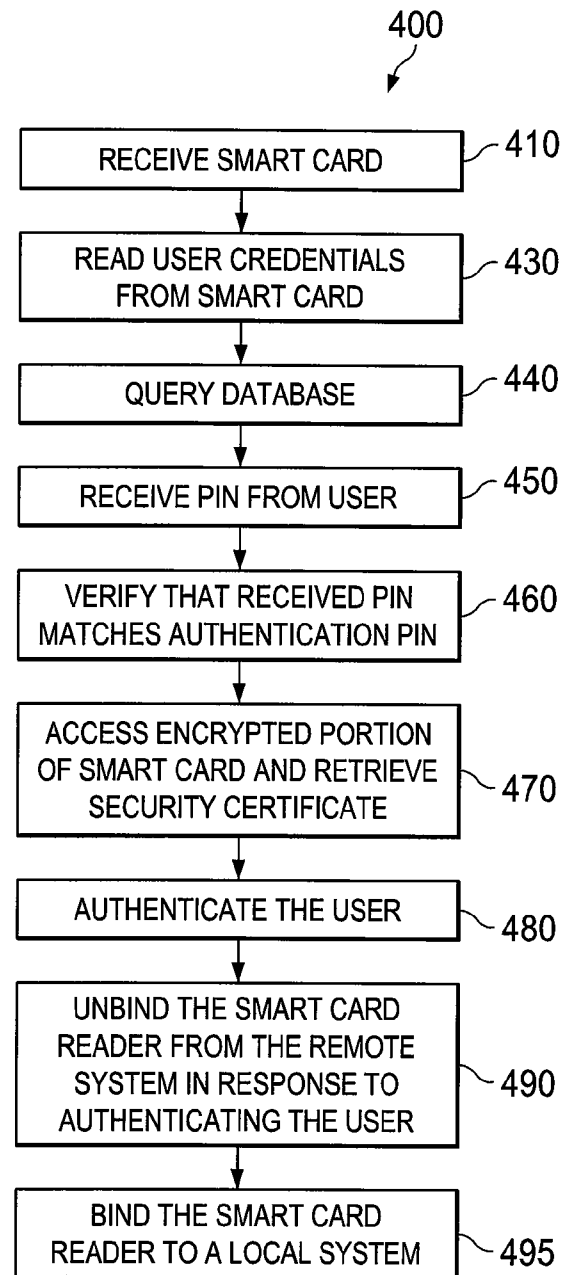


FIG. 6

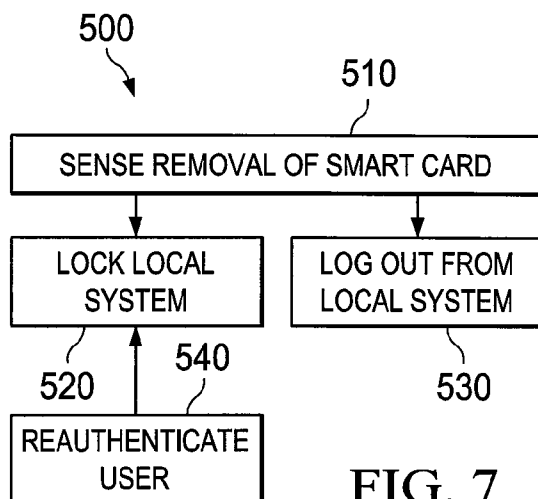


FIG. 7

A. CLASSIFICATION OF SUBJECT MATTER*G06F 15/16(2006.01)i, H04B 5/02(2006.01)i, G06K 17/00(2006.01)i, G06F 21/00(2006.01)i*

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC : G06F

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

Korean Utility models and applications for Utility models since 1975

Japanese Utility models and applications for Utility models since 1975

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

eKOMPASS(KIPO internal) "single sign on(SSO)", "smart card", "authenticate", "remote system", "local system", "share", "login"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ----- A	US 2006-0013393 A1(AZIM FERCHICHI et al.) 19 January 2006 See abstract; paragraphs [0092]-[0093], [0157], claims 1-18.	1, 9, 10 ----- 2-8, 11-15
A	US 2009-0007248 A1(MICHAEL KOVALESKI) 1 January 2009 See abstract; claims 1-12.	1-15
A	KR 10-2002-0039703 A(DREAMINTECH CORPORATION) 30 May 2002 See abstract; claims 1-6.	1-15
A	KR 10-2003-0075809 A(UDS CO., LTD.) 26 September 2003 See abstract; figures 1-3; claims 1-6.	1-15



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 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

25 NOVEMBER 2009 (25.11.2009)

Date of mailing of the international search report

25 NOVEMBER 2009 (25.11.2009)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

HAN, Seon Kyoung

Telephone No. 82-42-481-8523



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2009/036918

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0013393 A1	19.01.2006	AU 2000-64222 A1 EP 1254547 A1 EP 1254547 B1 US 07058180 B2 US 2003-0012382 A1 WO 2001-060013 A1	16.08.2000 06.11.2002 23.11.2005 06.06.2006 16.01.2003 16.08.2001
US 2009-0007248 A1	01.01.2009	None	
KR 10-2002-0039703 A	30.05.2002	None	
KR 10-2003-0075809 A	26.09.2003	None	