(19) DANMARK

(10) **DK/EP 3892023 T3**

(12) Oversættelse af europæisk patentskrift

Patent- og Varemærkestyrelsen

(51) Int.Cl.: ***H 04 W 12/069 (2021.01)*** ***H 04 L 9/00 (2022.01)*** ***H 04 L 9/08 (2006.01)*** ***H 04 L 9/32 (2006.01)*** ***H 04 L 9/40 (2022.01)*** ***H 04 W 4/80 (2018.01)***

(45) Oversættelsen bekendtgjort den: **2024-11-18**

(80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2024-08-21**

(86) Europæisk ansøgning nr.: **19893033.1**

(86) Europæisk indleveringsdag: **2019-12-06**

(87) Den europæiske ansøgnings publiceringsdag: **2021-10-13**

(86) International ansøgning nr.: **US2019064892**

(87) Internationalt publikationsnr.: **WO2020118161**

(30) Prioritet: **2018-12-06 US 201862776337 P**

(84) Designerede stater: **AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**

(73) Patenthaver: **Entrust Corporation, 1187 Park Place, Shakopee, MN 55379, USA**

(72) Opfinder: **MALLINSON, Michael, c/o Entrust, Inc. Two Lincoln Centre 5420 LBJ , Freeway, Suite 300, Dallas, TX 75240, USA**
REILLY, Ian, c/o Entrust, Inc. Two Lincoln Centre 5420 LBJ , Freeway, Suite 300, Dallas, TX 75240, USA
JAYAPRAKASH, Rathnavalli, c/o Entrust, Inc. Two Lincoln Centre 5420 LBJ , Freeway, Suite 300, Dallas, TX 75240, USA
LYNESS, Martin, c/o Entrust, Inc. Two Lincoln Centre 5420 LBJ , Freeway, Suite 300, Dallas, TX 75240, USA
GERLACH, Tim, c/o Entrust, Inc. Two Lincoln Centre 5420 LBJ , Freeway, Suite 300, Dallas, TX 75240, USA

(74) Fuldmægtig i Danmark: **Novagraaf Brevets, Bâtiment O2, 2 rue Sarah Bernhardt CS90017, F-92665 Asnières-sur-Seine cedex, Frankrig**

(54) Benævnelse: **ENKELTLOGON VED HJÆLP AF SMARTE LEGITIMATIONSOPLYSNINGER**

(56) Fremdragne publikationer:
EP-A1- 2 200 251
WO-A1-00/72506
KR-A- 20160 028 230
US-A1- 2003 007 641
US-A1- 2017 171 755
US-A1- 2017 324 568
US-A1- 2018 183 777
US-B1- 6 886 095

DESCRIPTION

Description

BACKGROUND

[0001] Applications configured to run natively on local computing devices (e.g., desktop or laptop computing devices, kiosk-type or terminal-type devices, etc., typically operating within a desktop computing environment) may require a high level of security, sometimes beyond simple username and password authentication. For example, such applications may require multifactor authentication, with a username/password authentication and an additional form of authentication (e.g., PIN or other code) or smart card or smart credential based authentication. For such systems, a mobile device may have a virtual smart card installed thereon, which facilitates authentication of the user for use of the local computing system.

[0002] In some instances, a user of such a local computing device may wish to use a browser application on that device to access remote applications (e.g., hosted by a remote server or offered on a software-as-a-service basis). However, that remote software may also be secure software requiring user authentication. Even in circumstances in which the remote software uses authentication credentials that are the same as those used for the application at the local computing system the remote software may require the user to re-authenticate him/herself within a browser window prior to accessing that software. This may also be the case where different authentication credentials are used for local and remote software, but both are managed using a similar credentialing process or credentialing mechanism, such as a smart card or other smart credential. This can be the case where an enterprise uses both local and remote or cloud applications. As such, there are a variety of instances in which separate authentication processes are required for both local and remote secure applications for the same user, and even in the same use session, causing significant inconvenience to that user.

[0003] The US Patent Application US 2017/171755 A1 discloses a Bluetooth authentication apparatus that authenticates a user and may issue a dynamic credential to a host computing system, which may be used to verify the user at an application, and provide access to an application at an application server to the user at the host computing system. The International Patent Application WO 00/72506 A1 discloses a method of securing communication for pairing two wireless devices with each other that includes use of exchanged device certificates and challenges, and signing of challenges using a receiving device's private key for subsequent validation using a public key provided to the challenge-issuing device.

SUMMARY

[0004] The present invention is defined in the independent claims. Preferred embodiments are defined in the dependent claims. The The present disclosure relates generally to facilitating sign-on to a plurality of secure applications with improved convenience. In general, the present disclosure provides for a single sign-on mechanism that allows a user who has been required to use a secure credential to access a first computing system, such as a local computing system, to subsequently access other computing resources (e.g., remote secure applications, such as cloud-based or server-based applications) that also require secure credential-based authentication. The subsequent authentication of the user based on that secure credential for subsequent access of other computing resources can be accomplished largely without requiring user involvement, due to coordination between a local computing system, a mobile device, and a remote authentication service.

[0005] In a first aspect, a method includes authenticating, at a first computing system, a user with a first secure application based on information received from a smart credential stored on a mobile device via a local wireless connection between the mobile device and the first computing system. The method further includes obtaining, via a browser of the first computing system, a remote challenge from a remote authentication service, and obtaining, via a browser of the first computing system, a mobile challenge from the mobile device. The method includes signing the mobile challenge with a private key of a public-private key pair at the first computing system, transmitting to the mobile device a version of the mobile challenge signed at the first computing system, the remote challenge, and a public key of the public-private key pair, and receiving, from the mobile device, a signed version of the remote challenge and a certificate indicating validation of the mobile challenge. The method further includes transmitting the signed version of the remote challenge to the remote authentication service, and, based on receiving an authentication result from the remote authentication service, granting access at the first computing system to a remote secure application via the browser.

[0006] In a second aspect, a method of authenticating a user for use of a plurality of secure applications includes establishing a local wireless connection between a mobile device and a first computing system. The method also includes, in response to receipt of a request from the first computing system, transmitting a mobile device challenge to the first computing system, and receiving a signed version of the mobile device challenge, a remote authentication challenge, and a public key of a public-private key pair from the first computing system, the signed version of the mobile device challenge being signed with a private key of the public-private key pair. The method further includes validating the signed version of the mobile device challenge using the public key, and signing the remote authentication challenge with the user credentials stored at the mobile device. The method includes transmitting a signed version of the remote authentication challenge and a certificate to the first computing system

[0007] In a third aspect, a system for facilitating authentication of a user with a plurality of secure applications is disclosed. The system includes a computing system. The computing system includes a local wireless communication interface, a network interface, a programmable circuit operatively connected to the local wireless communication interface and

the network interface, and a memory operatively connected to the programmable circuit. The memory stores instructions comprising a first secure application, a browser and a local wireless communication driver. The instructions are further configured to, when executed by the programmable circuit: authenticate, at a first computing system, a user with a first secure application based on information received from a mobile device via a local wireless connection between the mobile device and the first computing system; obtain a remote challenge from a remote authentication service; obtain, via the browser, a mobile challenge from the mobile device; sign the mobile challenge with a private key of a public-private key pair; transmit to the mobile device a signed version of the mobile challenge, the remote challenge, and a public key of the public-private key pair; receive, from the mobile device, a signed version of the remote challenge and a certificate indicating validation of the mobile challenge; transmit the signed version of the remote challenge to the remote authentication service; and based on receiving an authentication result from the remote authentication service, grant access to a remote secure application via the browser.

[0008] A variety of additional aspects will be set forth in the description that follows. The aspects can relate to individual features and to combinations of features. It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the broad inventive concepts upon which the embodiments disclosed herein are based.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The following drawings are illustrative of particular embodiments of the present disclosure and therefore do not limit the scope of the present disclosure. The drawings are not to scale and are intended for use in conjunction with the explanations in the following detailed description. Embodiments of the present disclosure will hereinafter be described in conjunction with the appended drawings, wherein like numerals denote like elements.

Figure 1 illustrates an example network within which aspects of the present disclosure can be implemented.

Figure 2 illustrates a detailed embodiment of a system within which single sign-on using a smart credential can be performed.

Figure 3 illustrates an example computing device useable to implement aspects of the present disclosure.

Figure 4 illustrates a method of facilitating sign-on to a second secure application based on sign-on to a first secure application, in an example embodiment.

Figure 5 illustrates a messaging sequence in which single sign-on can be accomplished upon an initial sign-on sequence being performed.

Figure 6 illustrates a messaging sequence in which a single sign-on session can be terminated

based on disconnection of a mobile device from a local computing device.

DETAILED DESCRIPTION

[0010] Various embodiments of the present invention will be described in detail with reference to the drawings, wherein like reference numerals represent like parts and assemblies throughout the several views. Reference to various embodiments does not limit the scope of the invention, which is limited only by the scope of the claims attached hereto. Additionally, any examples set forth in this specification are not intended to be limiting and merely set forth some of the many possible embodiments for the claimed invention.

[0011] As briefly described above, embodiments of the present invention are directed to methods and systems for signing on to secure applications in an efficient manner, e.g., by performing a single sign-on process that can be reused across different secure applications. In general, the present disclosure provides for a single sign-on mechanism that allows a user who has been required to use a secure credential to access a first computing system, such as a local computing system, to subsequently access other computing resources (e.g., remote secure applications, such as cloud-based or server-based applications) that also require secure credential-based authentication. The subsequent authentication of the user based on that secure credential for subsequent access of other computing resources can be accomplished largely without requiring user involvement. In some instances, the single sign-on mechanisms can be entirely or partially obscured from the user, to provide an appearance of seamless access of applications. Additionally, the methods and systems described herein can leverage a convenient secure authentication mechanism, such as a virtual smart card technology in which a mobile device stores a virtual smart card that is useable for local authentication of the user at a computing system via a short-range wireless (e.g., Bluetooth) connection.

[0012] Referring to Figure 1, an example network 10 within which aspects of the present disclosure can be implemented is illustrated. In the example network 10 shown, a first computing system 12 is operated by a user. The first computing system 12 can be, for example, a desktop or laptop computing system or a tablet or other mobile device that is directly operated by a user. The first computing system 12 has one or more applications installed thereon, including, for example, the operating system of the system, as well as user applications executed within the environment of the operating system. In use, the user seeks access to one or more applications. Such applications can include, e.g., the operating system of the computing device 12, a local application executing at the first computing system 12, or applications stored remotely from the first computing system 12. In example instances, the applications themselves, or the operating system, may require the user to be authenticated to allow access to the applications. Accordingly, in the context of the present disclosure any of a local operating system, local applications, and remote applications which each may apply

security policies or only permit access based on user authentication can be referred to as a secure application.

[0013] In the embodiment shown, the first computing system 12 is communicatively connected to a mobile device 14 via a short-range wireless network. The short range wireless network can be any of a variety of such short-range networks, one example of which is Bluetooth, which may include both traditional Bluetooth and Bluetooth Low Energy (BLE) variants. Other short range wireless communication protocols, such as Near Field Communication (NFC) could be used in alternative embodiments. Alternatively, the mobile device 14 can be connected to the first computing system by an alternative connection, e.g., by way of an ad-hoc WiFi network, or by a wired connection. The mobile device 14 can be implemented to host a smart credential, such as the Mobile Smart Credential provided by Entrust Datacard of Shakopee, Minnesota.

[0014] The first computing system 12 is also connected to a remote computing system 16 via a network 18, such as the internet. The remote computing system 16 may be, as shown in Figure 1, a cloud server. Alternatively, the remote computing system may be a remote enterprise server or other remote computing system that is communicatively connected to the first computing system 12 via any type of network, including the Internet, as well as various other LAN, WAN or other networks.

[0015] In the example shown, the remote computing system 16 hosts one or more secure applications that can be accessible from the first computing system 12. In example instances, the one or more secure applications resident on the remote computing system 16 can be accessible at the first computing system 12 via a browser application.

[0016] In the example shown, a remote authentication service 22 is also communicatively accessible from the first computing system 12. The remote authentication service 22 is generally accessible from the first computing system 12, and may be redirected by remote computing system 16 to provide authorization to access the one or more secure applications hosted thereon. In an example embodiment, the remote authentication service can be implemented using a secure remote authentication service refererred to as the INTELLITRUST portal provided by Entrust Datacard of Shakopee, Minnesota.

[0017] Figure 2 illustrates a detailed embodiment of a system 100 within which single sign-on using a smart credential can be performed. The system 100 is implemented with particular implementations of the computing systems of Figure 1, including, e.g., mobile device 14, first computing device 12 (shown as a desktop computing device), a remote computing system 16 (shown as a cloud or server device), and a remote authentication service 22.

[0018] In the embodiment shown, the mobile device 14 stores a mobile smart card 102 that has mobile credentials 104 embodied therein. The mobile credentials 104 can include, for example, unique information associated with a user, or instructions that can generate unique user information in response to a user logging in to an application on the mobile device 12 that enables the mobile smart card 102. In example embodiments, the mobile smart card 102 can

be implemented using a Mobile Smart Credential provided by Entrust Datacard of Shakopee, Minnesota.

[0019] In the example shown, the mobile device 14 also has a short range wireless interface, shown as Bluetooth interface 106. Other short range wireless interfaces are available as well (e.g., an ad-hoc WiFi communication connection between two devices). In general the short range wireless interface can be an interface which is configured to either automatically or manually connect to a local device (such as desktop device 12) when within wireless communication range of that device.

[0020] In the example shown, the desktop device 12 includes a desktop secure application 202, a browser 204, a Bluetooth driver 206, authentication keys 208, a network interface 210, and a Bluetooth interface 212. The desktop secure application 202 generally corresponds to an application that requires authentication for access that is executable on the desktop device 12. For example the desktop secure application 202 could include an operating system, a local application requiring authentication, or a hosted application at the desktop device 12 that also requires authentication. The browser 204 includes in the example shown an authentication user interface 205. The authentication user interface 205 may be code that executes within the browser 204, such as Javascript or other code capable of executing a process for authenticating a user remotely. The authentication user interface can be displayed within the browser 204 upon the browser being redirected to an authentication system such as authentication device 22. The authentication user interface 205 can be used to remotely authenticate a user in association with use of either the desktop secure application 202 or a remote secure application, such as remote secure application 302 on server device 16.

[0021] In the example shown the Bluetooth interface 212 allows for a local wireless connection to a corresponding Bluetooth interface 106 of mobile device 14. In operation, Bluetooth interface 212 or Bluetooth interface 106 will scan a local wireless area and recognize the corresponding Bluetooth interface. Accordingly when the mobile device 14 is in proximity to desktop device 12, the mobile device 14 and the desktop device 12 may automatically connect via Bluetooth.

[0022] In the embodiment shown, the Bluetooth driver 206 includes a Bluetooth single sign-on service 207. The Bluetooth single sign-on service 207 exchanges data between an authentication user interface 205 and the mobile smartcard 102 via Bluetooth interfaces 212, 106. Details regarding an exchange of messages between the authentication user interface 205, the mobile smartcard 102 and a remote authentication service 402 are described in below in conjunction with Figures 4-5.

[0023] The authentication keys 208 are stored at the desktop device 12 for example via the Bluetooth single sign-on service 207 or browser 204. Details regarding the use of the authentication keys 208 for effectuating the single sign-on processes of the present disclosure are also described below in conjunction with Figures 4-6.

[0024] Also in the example embodiment shown a server device 16 includes a remote secure application 302 and a network interface 304. The remote secure application 302 can be any of a variety of remote applications accessible via the browser 204. For example the remote secure application 302 can be a cloud-based or server-based application provided "as a service" such as an application hosted within Office365 or Salesforce server/cloud ecosystems.

[0025] As illustrated in Figure 2, the desktop device 12 is communicatively connected to server device 16 and authentication device 22 via a network 18, such as the Internet. These devices are interconnected via network interfaces 210, 304, and 404. The devices may be remotely located from each other or two or more of the devices may be co-located.

[0026] In use, connection of the mobile device 14 to the desktop device 12 via the Bluetooth connection may allow access to the desktop secure application 202. The authentication service 402 can be accessed via the browser 204 to authenticate the user at the desktop device 12 for access to the remote secure application 302. Because the mobile smartcard 102 has previously been used to accesses the desktop secure application 202, the authentication service 402 and mobile smart card 102 may cooperate via the authentication user interface 205 and Bluetooth single sign-on service 207 to authenticate the user for use of the remote secure application 302 without requiring further user interaction.

[0027] Referring now to Figure 3, a computing device 500 is shown, with which aspects of the present disclosure can be implemented. The computing device 500 can be used, for example, to implement any of the mobile device 14, desktop device 12, or cloud/server devices 16, 22 of Figures 1-2.

[0028] In the example of Figure 3, the computing device 500 includes a memory 502, a processing system 504, a secondary storage device 506, a network interface card 508, a video interface 510, a display unit 512, an external component interface 514, and a communication medium 516. The memory 502 includes one or more computer storage media capable of storing data and/or instructions. In different embodiments, the memory 502 is implemented in different ways. For example, the memory 502 can be implemented using various types of computer storage media, and generally includes at least some tangible media. In some embodiments, the memory 502 is implemented using entirely non-transitory media.

[0029] The processing system 504 includes one or more processing units, or programmable circuits. A processing unit is a physical device or article of manufacture comprising one or more integrated circuits that selectively execute software instructions. In various embodiments, the processing system 504 is implemented in various ways. For example, the processing system 504 can be implemented as one or more physical or logical processing cores. In another example, the processing system 504 can include one or more separate microprocessors. In yet another example embodiment, the processing system 504 can include an application-specific integrated circuit (ASIC) that provides specific functionality. In yet another example, the processing system 504 provides specific functionality by using an ASIC and by executing computer-executable instructions.

[0030] The secondary storage device 506 includes one or more computer storage media. The secondary storage device 506 stores data and software instructions not directly accessible by the processing system 504. In other words, the processing system 504 performs an I/O operation to retrieve data and/or software instructions from the secondary storage device 506. In various embodiments, the secondary storage device 506 includes various types of computer storage media. For example, the secondary storage device 506 can include one or more magnetic disks, magnetic tape drives, optical discs, solid-state memory devices, and/or other types of tangible computer storage media.

[0031] The network interface card 508 enables the computing device 500 to send data to and receive data from a communication network. In different embodiments, the network interface card 508 is implemented in different ways. For example, the network interface card 508 can be implemented as an Ethernet interface, a token-ring network interface, a fiber optic network interface, a wireless network interface (e.g., WiFi, WiMax, etc.), or another type of network interface.

[0032] The video interface 510 enables the computing device 500 to output video information to the display unit 512. The display unit 512 can be various types of devices for displaying video information, such as an LCD display panel, a plasma screen display panel, a touch-sensitive display panel, an LED screen, a cathode-ray tube display, or a projector. The video interface 510 can communicate with the display unit 512 in various ways, such as via a Universal Serial Bus (USB) connector, a VGA connector, a digital visual interface (DVI) connector, an S-Video connector, a High-Definition Multimedia Interface (HDMI) interface, or a DisplayPort connector.

[0033] The external component interface 514 enables the computing device 500 to communicate with external devices. For example, the external component interface 514 can be a USB interface, a FireWire interface, a serial port interface, a parallel port interface, a PS/2 interface, and/or another type of interface that enables the computing device 500 to communicate with external devices. In various embodiments, the external component interface 514 enables the computing device 500 to communicate with various external components, such as external storage devices, input devices, speakers, modems, media player docks, other computing devices, scanners, digital cameras, and fingerprint readers.

[0034] The communication medium 516 facilitates communication among the hardware components of the computing device 500. The communications medium 516 facilitates communication among the memory 502, the processing system 504, the secondary storage device 506, the network interface card 508, the video interface 510, and the external component interface 514. The communications medium 516 can be implemented in various ways. For example, the communications medium 516 can include a PCI bus, a PCI Express bus, an accelerated graphics port (AGP) bus, a serial Advanced Technology Attachment (ATA) interconnect, a parallel ATA interconnect, a Fiber Channel interconnect, a USB bus, a Small Computing system Interface (SCSI) interface, or another type of communications medium.

[0035] The memory 502 stores various types of data and/or software instructions. The memory 502 stores a Basic Input/Output System (BIOS) 518 and an operating system 520. The BIOS 518 includes a set of computer-executable instructions that, when executed by the processing system 504, cause the computing device 500 to boot up. The operating system 520 includes a set of computer-executable instructions that, when executed by the processing system 504, cause the computing device 500 to provide an operating system that coordinates the activities and sharing of resources of the computing device 500. Furthermore, the memory 502 stores application software 522. The application software 522 includes computer-executable instructions, that when executed by the processing system 504, cause the computing device 500 to provide one or more applications. The memory 502 also stores program data 524. The program data 524 is data used by programs that execute on the computing device 500.

[0036] Although particular features are discussed herein as included within an electronic computing device 500, it is recognized that in certain embodiments not all such components or features may be included within a computing device executing according to the methods and systems of the present disclosure. Furthermore, different types of hardware and/or software systems could be incorporated into such an electronic computing device.

[0037] In accordance with the present disclosure, the term computer readable media as used herein may include computer storage media and communication media. As used in this document, a computer storage medium is a device or article of manufacture that stores data and/or computer-executable instructions. Computer storage media may include volatile and nonvolatile, removable and non-removable devices or articles of manufacture implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules, or other data. By way of example, and not limitation, computer storage media may include dynamic random access memory (DRAM), double data rate synchronous dynamic random access memory (DDR SDRAM), reduced latency DRAM, DDR2 SDRAM, DDR3 SDRAM, solid state memory, read-only memory (ROM), electrically-erasable programmable ROM, optical discs (e.g., CD-ROMs, DVDs, etc.), magnetic disks (e.g., hard disks, floppy disks, etc.), magnetic tapes, and other types of devices and/or articles of manufacture that store data. Communication media may be embodied by computer readable instructions, data structures, program modules, or other data in a modulated data signal, such as a carrier wave or other transport mechanism, and includes any information delivery media. The term "modulated data signal" may describe a signal that has one or more characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media may include wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, radio frequency (RF), infrared, and other wireless media.

[0038] It is noted that, in some embodiments of the computing device 500 of Figure 3, the computer-readable instructions are stored on devices that include non-transitory media. In particular embodiments, the computer-readable instructions are stored on entirely non-transitory media.

[0039] Referring now to Figure 4, a method 600 of facilitating sign-on to a second secure application based on sign-on to a first secure application is shown, in an example embodiment. The example method 600 can be performed, for example, using the systems and networks described above in connection with Figures 1-3.

[0040] In the example embodiment shown, the method includes, at 602, authenticating a user with a first secure application. This authentication may be authentication of a local application, such as a local operating system or application-level program. The authentication can be performed in response to a user attempting to access the first secure application, or in response to connection of a mobile device to the computing system on which the first secure application resides, such as a local computing device.

[0041] In the embodiment shown, the method includes, at 604, accessing a remote secure application or remote authentication service. Accessing the remote authentication service may include, for example, receiving at a browser of a local computing device a redirection from a remote secure application to the remote authentication service for purposes of authentication and access to the remote secure application.

[0042] In the embodiment shown, the method includes, at 606, receiving a challenge from the remote authentication service. This may be performed, for example, in response to transmitting a request for the challenge from a local computing device to the remote authentication service.

[0043] In the embodiment shown, the method includes, at 608, obtaining a challenge from the mobile device as well. This may be performed, for example, by issuing a request from a browser or authentication user interface to a Bluetooth single sign-on service, which in turn relays that request to the mobile device credential. The mobile device can either return a stored challenge, or create a challenge and store that challenge, returning it to the browser via the Bluetooth single sign-on service.

[0044] In the embodiment shown, the method includes, at 610, signing the received mobile challenge with a private key. The private key maybe, for example, a private key of a public/private key pair that is previously stored at the local computing device or generated at the local computing device in response to receiving the challenge. The public/private key pair may be generated by either the authentication user interface 205 or Bluetooth single sign-on service 207. The public private key pair may be included within authentication keys 208 as seen in Figure 2.

[0045] In the embodiment shown, the method includes, at 612, providing the signed mobile challenge, the challenge received from the authentication service, and the public key of the public-private key pair to the mobile device. In particular, the signed challenge and the public key can be provided to the mobile credential (e.g., mobile smart card 102).

[0046] In the embodiment shown, the method includes, at 614, validating the signed challenge at the mobile device, and in particular at the mobile smart card 102. Validating the challenge can include use of the public key that is generated as part of the public/private key pair at the authentication user interface and/or browser. It can also include, for example, requesting user authentication credentials at the mobile device 14 to register the received public key, and subsequently registering the public key at the mobile smart card 102.

[0047] The method also includes, in the embodiment shown, (and also at 614), signing the authentication service challenge with user credentials that are either are stored in the mobile smart card 102 or received from a user (for example, user authentication credentials as requested above).

[0048] In the embodiment shown, the method includes, at 616, returning the signed authentication service challenge to the first computing device and validating the challenge signed using the user credentials by sending the user-signed version of the authentication service challenge to the remote authentication service 402.

[0049] In the embodiment shown, the method includes, at 618, receiving a redirection from the remote authentication service that redirects a browser of the first computing device to the remote secure application. The redirection from the remote authentication service indicates to the browser that the user is authenticated to access the remote secure application. Accordingly, the user may, via the browser, transmit requests to the remote secure application.

[0050] As further seen in Figure 4, at 620, the connection to both the local secure application(s) and remote secure application(s) will be maintained so long as the connection between mobile device 14 and local computing device 12 is maintained. That is, in some embodiments, the Bluetooth single sign-on service 207 will monitor connection status of a Bluetooth connection to the mobile device 14. If and when the connection no longer exists (e.g., a user turns off Bluetooth, removes the mobile device from the vicinity of the local computing system, etc.) a secure connection termination process is automatically initiated to close both local and remote secure application connection sessions in a seamless manner without causing data loss. One example messaging sequence useable to accomplish this is illustrated in further detail below in connection with Figure 6.

[0051] Referring to Figure 4 overall, it is noted that after the user is authenticated at both the mobile device and the first secure application, authenticating the user at the remote secure application may require a browser to be redirected to an authentication service, but does not require the user to reenter his or her user credentials. Accordingly, the user experience is simplified.

[0052] Figure 5 illustrates a messaging sequence 700 in which single sign-on can be accomplished upon an initial sign-on sequence being performed. The messaging sequence 700 generally reflects a communication sequence occurring after the user has been authenticated for use of local secure application at a first computing device 12 of Figures 1-2.

Generally, the messaging sequence 700 is performed on a mobile smartcard 102, a Bluetooth single sign-on service 207, a browser 204, and a remote authentication service 402.

[0053] In the example shown, a secure channel is established between the mobile smartcard 102 and Bluetooth single sign-on service 207. A user, seeking to access a remote secure application, will initiate an authentication process within a browser 204. When the user accesses the remote secure application, the user may be redirected to an authentication service 402. To initiate authentication via the remote authentication service 402, the authentication user interface 205 presented within browser 204 transmits a request for a challenge to the remote authentication service 402. In the example shown, the remote authentication service 402 will create and store a challenge, and return the challenge to the browser 204.

[0054] The authentication user interface 205 within browser 204 also transmits a request to the mobile device 14 (e.g., to mobile smart card 102) to obtain a challenge from the mobile device. The request can be passed through the Bluetooth single sign-on service 207. In the example shown, the mobile device, and in particular the mobile smart card 102, will create and store a mobile challenge, which is returned to the browser 204 via the Bluetooth single sign-on service 207. It is noted that the order in which challenges are requested from the authentication service 402 and mobile smart card 102 may be reversed or altered in alternative embodiments.

[0055] Upon acquisition of the remote authentication service challenge and the mobile challenge, if the authentication user interface 205 is able to obtain a key pair from local storage, it will do so. If no key pair exists, the authentication user interface 205 and/or browser 204 may generate and store a new public-private key pair. The received mobile challenge will then be signed by the authentication user interface with the private key of the key pair. An authentication request including the signed mobile challenge, the remote authentication service challenge, and the public key of the public-private key pair are provided to the Bluetooth single sign-on service 207. The Bluetooth single sign-on service 207 will relay the request to the mobile smart card 102 to validate the signed mobile challenge. Alongside the request, the Bluetooth single sign on service 207 will also provide the public key and the remote authentication service challenge.

[0056] At the mobile smart card 102, an assessment is made to determine whether the public key is registered with the mobile smartcard. If the public key is not registered, the user may be prompted to enter user authentication information, for example a PIN code, into a user interface of the mobile device. Once the user successfully enters a PIN code the public key is registered within the mobile smart card 102. The mobile smartcard 102 then validates the challenge signature on the mobile challenge using the public key received and registered. The mobile smart card 102 will then sign the remote authentication service challenge with the user credentials stored in the mobile smart card 102. The mobile smart card 102 will then return to the authentication user interface 205 the signed remote authentication service challenge and a certificate. In particular, the signed challenge and the certificate are provided to the Bluetooth

single sign-on service 207.

[0057] In the embodiment shown, the Bluetooth single sign-on service 207 will then relay the user-signed remote authentication service challenge and the certificate to the browser 204, for use by the authentication user interface 205. The authentication user interface 205 will then relay the user-signed remote authentication service challenge to the authentication service 402, where it can be authenticated. An authentication result is then sent from the authentication service 402 back to the browser 204. This may take the form of a redirection back to the remote secure application, thereby allowing for subsequent requests to be passed directly to the now-authenticated remote secure application. In example embodiments, the authentication result can take the form of an authentication token received at the browser 204 for use in accessing a remote secure application, e.g., via SAML or OIDC-based requests.

[0058] Referring to Figures 1-5 generally, it is noted that only in the case that the public key of the browser is not registered will a user typically be required to provide further user authentication information (e.g., a PIN code) into the mobile device. Once a public key has been registered at the mobile smart card 102, the browser 204 and the local computing device 12 generally have established a registered relationship with the mobile smart card 102, and therefore no re-entry would typically be required. Accordingly, the entire sequence of operations as illustrated in Figure 5 may be obscured to the user, and will appear as a single sign-on service that allows access to a remote secure application based on previous authentication of the user at a local secure application. In this way, the user may have his or her secure access to desktop applications via the mobile smart card seamlessly extended to remote applications, including cloud applications, which the user may wish to access, without a need to provide further user input to effectuate authentication for each new secure application where user re-entry of authentication information would otherwise be required. Still further, because mutual challenges are requested from the mobile device and the remote authentication service from a local computing device, end-to-end security from the mobile device to the local computing device to the remote authentication service can be ensured.

[0059] Referring now to Figure 6, a messaging sequence 800 in which single sign-on session can be terminated in response to disconnection of a mobile device from a local computing device (e.g., disconnection of a Bluetooth connection) is shown. The messaging sequence 800 generally reflects a communication sequence occurring after a single sign-on sequence has been performed, such as the one in Figure 5. Generally, the messaging sequence 800 is performed on a mobile smart card 102, a Bluetooth single sign-on service 207, a local secure application 202, a browser 204, a remote authentication service 402, and a remote secure application 302.

[0060] In the example shown, a mobile smart card 102 may disconnect from a local computer 14, e.g., by having its Bluetooth connection disconnected. In this instance, a Bluetooth single sign-on service 207 can detect the disconnection of the mobile smart card 102, and will transmit a logout command to the local secure application 202 as well as a logout command, via the browser 204, to the remote authentication service 402. The remote authentication

service will cause the user's session to log out, thereby terminating the user's valid credentials for access to remote secure applications; additionally, the remote authentication service 402 can transmit a logout command to the remote secure application(s) 302 that utilize the remote authentication service 402. This causes the remote secure applications to log out (e.g., saving work before sessions/connections are terminated).

[0061] Accordingly, based on the sequence 800 seen in Figure 6, upon disconnection of the mobile device from a local computing system, not only will a local secure application be caused to log out, but a remote secure application will be caused to log out seamlessly as well. Accordingly, not only is the sign-on process performed in a manner that is obscured to the user, the log-out process is also performed without a requirement of additional user action.

[0062] Although the present disclosure has been described with reference to particular means, materials and embodiments, from the foregoing description, one skilled in the art can easily ascertain the essential characteristics of the present disclosure and various changes and modifications may be made to adapt the various uses and characteristics without departing from the scope of the present invention as set forth in the following claims.

REFERENCES CITED IN THE DESCRIPTION

Cited references

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US2017171755A1 [0003]
- WO0072506A1 [0003]

Patentkrav

1. Fremgangsmåde omfattende:

godkendelse (602) ved et første computersystem (12, 204-206) af en bruger med en første sikker applikation (202, 302) baseret på oplysninger modtaget fra en mobil enhed (14, 102) via en lokal trådløs forbindelse mellem den mobile enhed og det første computersystem,

opnåelse (606) via en browser (204) i det første computersystem af en fjernudfordring fra en fjerngodkendelsestjeneste (402),

opnåelse (608) via en browser i det første computersystem af en mobil udfordring fra den mobile enhed,

signering (610) af den mobile udfordring med en privat nøgle til et offentlig-privat nøglepar ved det første computersystem,

transmission af den mobile udfordring (612) til den mobile enhed signeret ved det første computersystem, fjernudfordringen og en offentlig nøgle til det offentlig-private nøglepar,

modtagelse af fjernudfordringen (614-616) fra den mobile enhed signeret af den mobile enhed og et certifikat, der angiver validering af mobiludfordringen ved hjælp af den offentlige nøgle,

transmission (616) af fjernudfordringen signeret af den mobile enhed til fjerngodkendelsestjenesten, og

baseret på modtagelse af et godkendelsesresultat fra fjerngodkendelsestjenesten, der giver adgang (618) ved det første computersystem til en sikker fjernapplikation via browseren.

2. Fremgangsmåde ifølge krav 1, hvor de oplysninger, der modtages fra den mobile enhed, omfatter PKI-legitimationsoplysninger.

3. Fremgangsmåde ifølge krav 1, der yderligere omfatter hentning af det offentlig-private nøglepar fra lageret ved det første computersystem.

4. Fremgangsmåde ifølge krav 1, yderligere omfattende generering af det offentlig-private nøglepar ved den første computerenhed.

5. Fremgangsmåde ifølge krav 1, hvor tildeling af adgang ved det første computersystem til den eksterne sikre applikation sker uden at kræve brugergenindtastning af godkendelseslegitimationsoplysninger på enten den mobile enhed eller det første computersystem.

6. Fremgangsmåde ifølge krav 1, som yderligere omfatter: adgang til en fjernvært, der er tilknyttet den eksterne sikre applikation, og modtagelse af et omdirigeringslink fra fjernværten, der omdirigerer browseren til fjerngodkendelsestjenesten, hvor fjerngodkendelsestjenesten er adskilt fra fjernværten.

7. Fremgangsmåde ifølge krav 1, hvor den første sikre applikation omfatter en lokal godkendelsesapplikation, der kan bruges til at give adgang til et operativsystem i det første computersystem, og hvor en godkendelsestjeneste hostet inden for en webside i browseren er konfigureret til at signere udfordringen med den private nøgle.

8. Fremgangsmåde ifølge krav 1, hvor en Bluetooth-enkeltlogontjeneste indlejret i en Bluetooth-driver på det første computersystem udveksler data mellem browseren og den mobile enhed, og hvor transmission af den brugersignerede version af udfordringen udføres via Bluetooth-enkeltlogontjenesten.

9. Fremgangsmåde ifølge krav 1, som yderligere omfatter:

detektering af frakobling af den lokale trådløse forbindelse mellem den mobile enhed og det første computersystem,

som reaktion på detektering af frakobling, afslutning af en godkendt session med den første sikre applikation og transmission af en meddelelse til fjerngodkendelsestjenesten for at afslutte en fjernsession, der giver adgang til den eksterne sikre applikation ved det første computersystem.

10. Fremgangsmåde til godkendelse af en bruger med henblik på anvendelse af en flerhed af sikre applikationer, idet fremgangsmåden omfatter:

etablering (602) af en lokal trådløs forbindelse mellem en mobil enhed (14) og et første computersystem (12),

som svar på modtagelse af en anmodning fra det første computersystem, transmission ved hjælp af den mobile enhed (608) af en mobil udfordring til det første computersystem,

modtagelse på den mobile enhed (612) af den mobile udfordring signeret ved det første computersystem, en fjerngodkendelsesudfordring og en offentlig nøgle til et offentlig-privat nøglepar fra det første computersystem, hvor den mobile udfordring signeret ved det første computersystem med en privat nøgle i parret offentlig-privat nøgle, idet fjerngodkendelsesudfordringen er en udfordring, der modtages ved det første computersystem fra et fjerncomputersystem,

validering af den mobile enheds udfordring på den mobile enhed (612) ved hjælp af den offentlige nøgle,

signering på den mobile enhed (614) af fjerngodkendelsesudfordringen med de brugeroplysninger, der er gemt på den mobile enhed, og

transmission via den mobile enhed (616) af den eksterne godkendelsesudfordring signeret af den mobile enhed, og et certifikat, der angiver validering af mobiludfordringen ved hjælp af den offentlige nøgle til det første computersystem.

11. Fremgangsmåde ifølge krav 10, som yderligere omfatter:

fastslåelse af, hvorvidt den offentlige nøgle er registreret på den mobile enhed, og

når det fastslås, at den offentlige nøgle ikke er registreret på den mobile enhed, anmodning til brugeren om godkendelsesoplysninger inden registrering af den offentlige nøgle, hvor godkendelsesoplysningerne omfatter en pinkode.

12. Et system til at lette godkendelse af en bruger med en flerhed af sikre applikationer, idet systemet omfatter:

et computersystem (12, 500), der omfatter:

en lokal trådløs kommunikationsgrænseflade (212),

en netværksgrænseflade (210),

et programmerbart kredsløb (504), der operativt er forbundet til den lokale trådløse kommunikationsgrænseflade og netværksgrænsefladen,

en hukommelse (502), der operativt er forbundet til det programmerbare kredsløb og lagrer instruktioner, der omfatter en første sikker applikation (202), en browser (204) og en lokal trådløs kommunikationsdriver (206), idet instruktionerne yderligere konfigureres til, når de udføres af det programmerbare kredsløb:

godkendelse (602) ved computersystemet af en bruger med en første sikker applikation baseret på oplysninger modtaget fra en mobil enhed via en lokal trådløs forbindelse mellem den mobile enhed og det første computersystem,

opnåelse (606) af en fjernudfordring fra en fjerngodkendelsestjeneste,

opnåelse (608) via browseren af en mobil udfordring fra den mobile enhed,

signering (610) af mobiludfordringen med en privat nøgle til et offentlig-privat nøglepar,

transmission (612) til mobilenheden af den mobile udfordring signeret af computersystemet, fjernudfordringen og en offentlig nøgle til det offentlig-private nøglepar,

modtagelse (614-616) fra mobilenheden af den eksterne udfordring signeret af den mobile enhed, og et certifikat, der angiver validering af mobiludfordringen på mobilenheden ved hjælp af den offentlige nøgle,

transmission (616) af fjernudfordringen signeret af den mobile enhed til fjerngodkendelsestjenesten, og

baseret på modtagelse af et godkendelsesresultat fra fjerngodkendelsestjenesten, levering af adgang (618) til et eksternt sikkert program via browseren.

13. System ifølge krav 12, hvor den lokale trådløse kommunikationsgrænseflade omfatter en Bluetooth-grænseflade, og den lokale trådløse kommunikationsdriver omfatter en Bluetooth-driver, idet systemet yderligere omfatter en mobil enhed kommunikativt forbundet til computersystemet via Bluetooth-grænsefladen.

14. System ifølge krav 12, der yderligere omfatter fjernidentifikationstjenesten, hvor modtagelse af et godkendelsesresultat omfatter modtagelse af en omdirigering fra fjerngodkendelsestjenesten til den anden sikre applikation, idet den anden sikre applikation er placeret fjernt fra computersystemet.

DRAWINGS

Drawing

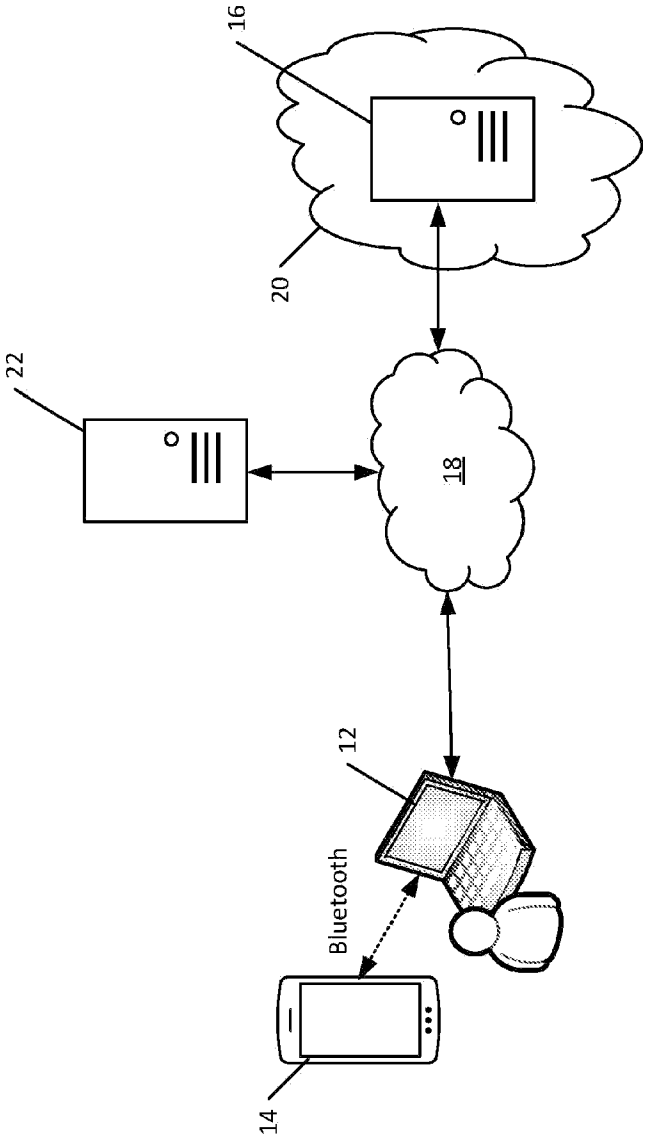

FIG. 1

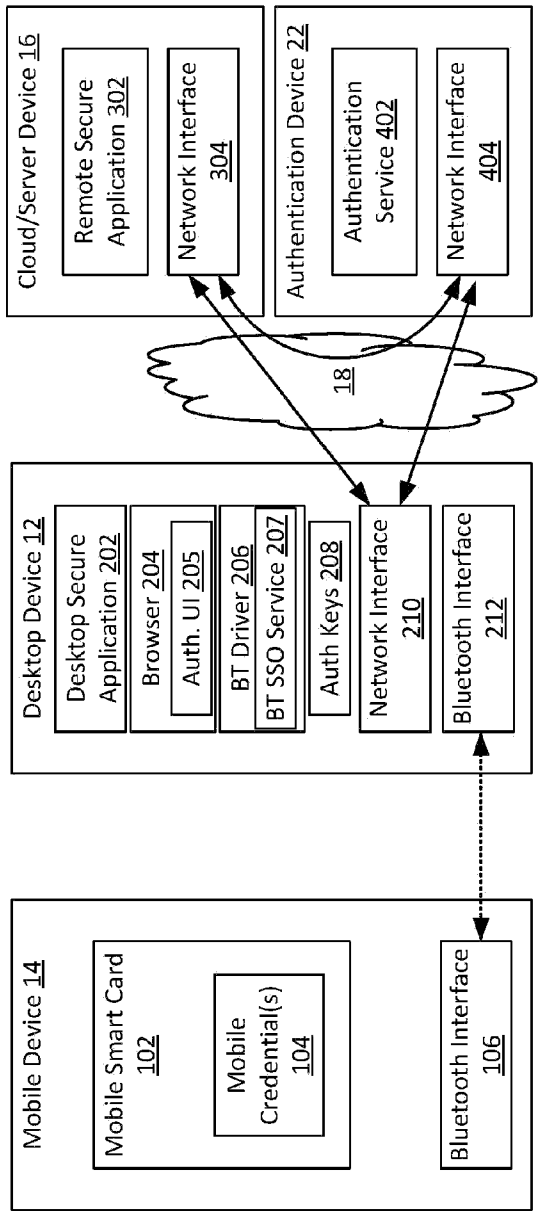
Cloud/Server Device 16
Remote Secure Application 302
Network Interface 304
Authentication Device 22
Authentication Service 402
Network Interface 404
18
Desktop Device 12
Desktop Secure Application 202
Browser 204
Auth. UI 205
BT Driver 206
BT SSO Service 207
Auth Keys 208
Network Interface 210
Bluetooth Interface 212
Mobile Device 14
Mobile Smart Card 102
Mobile Credential(s) 104
Bluetooth Interface 106
100

FIG. 2

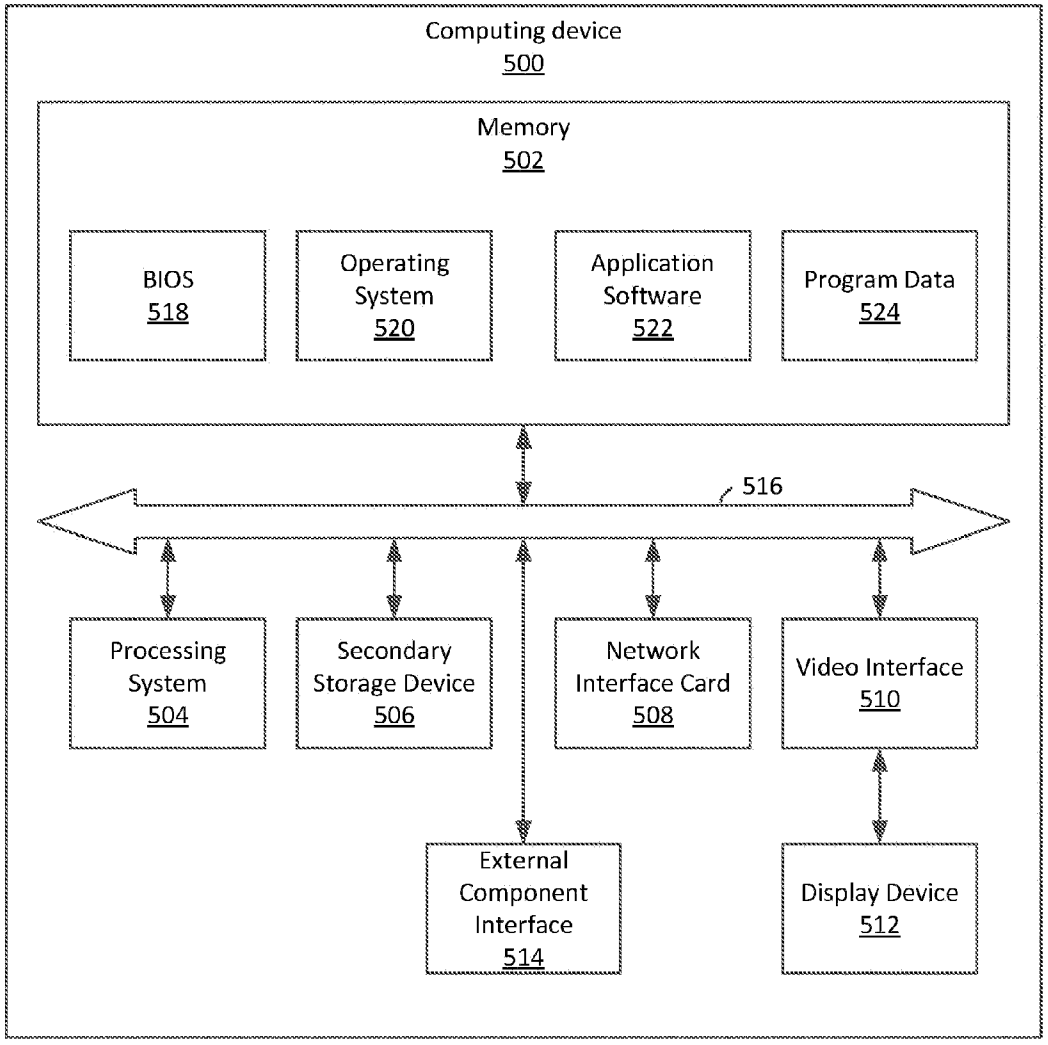
Computing device
500
Memory
502
BIOS
518
Operating System
520
Application Software
522
Program Data
524
516
Processing System
504
Secondary Storage Device
506
Network Interface Card
508
Video Interface
510
External Component Interface
514
Display Device
512

FIG. 3

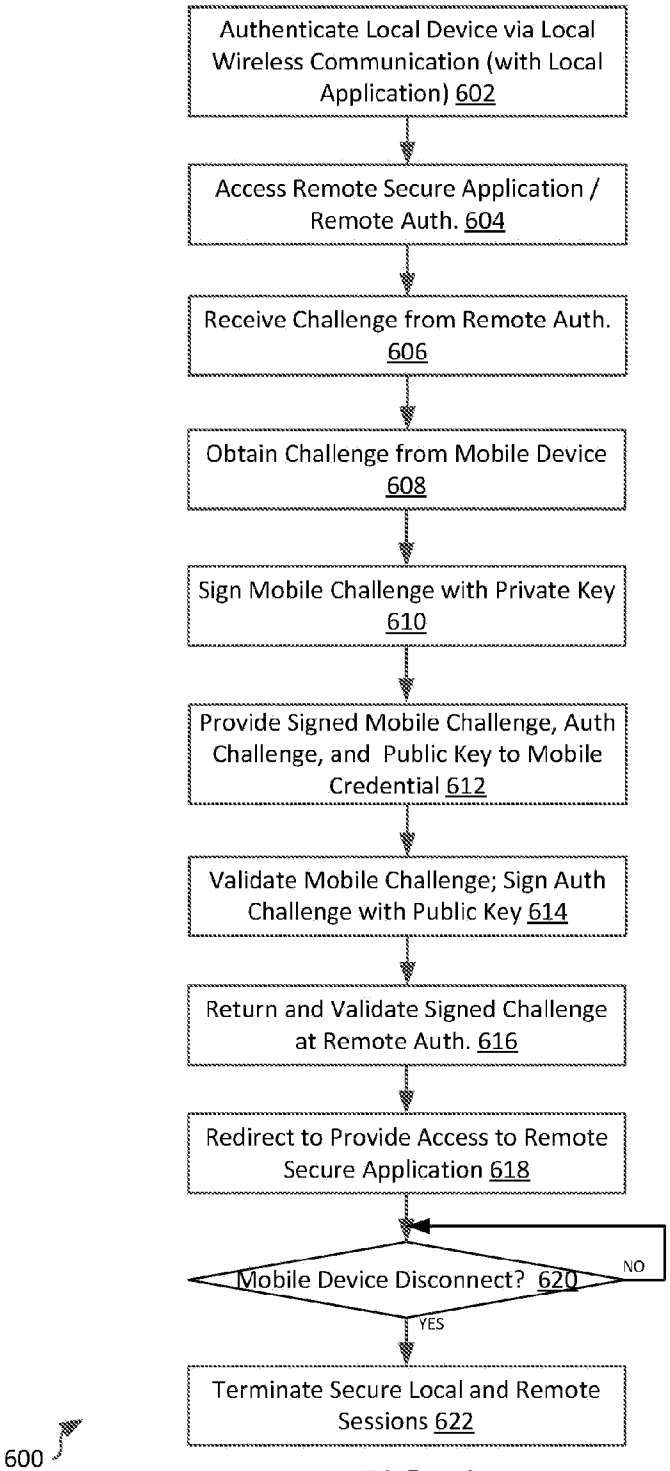
Authenticate Local Device via Local Wireless Communication (with Local Application) 602
Access Remote Secure Application / Remote Auth. 604
Receive Challenge from Remote Auth. 606
Obtain Challenge from Mobile Device 608
Sign Mobile Challenge with Private Key 610
Provide Signed Mobile Challenge, Auth Challenge, and Public Key to Mobile Credential 612
Validate Mobile Challenge; Sign Auth Challenge with Public Key 614
Return and Validate Signed Challenge at Remote Auth. 616
Redirect to Provide Access to Remote Secure Application 618
Mobile Device Disconnect? 620
NO
YES
Terminate Secure Local and Remote Sessions 622
600

FIG. 4

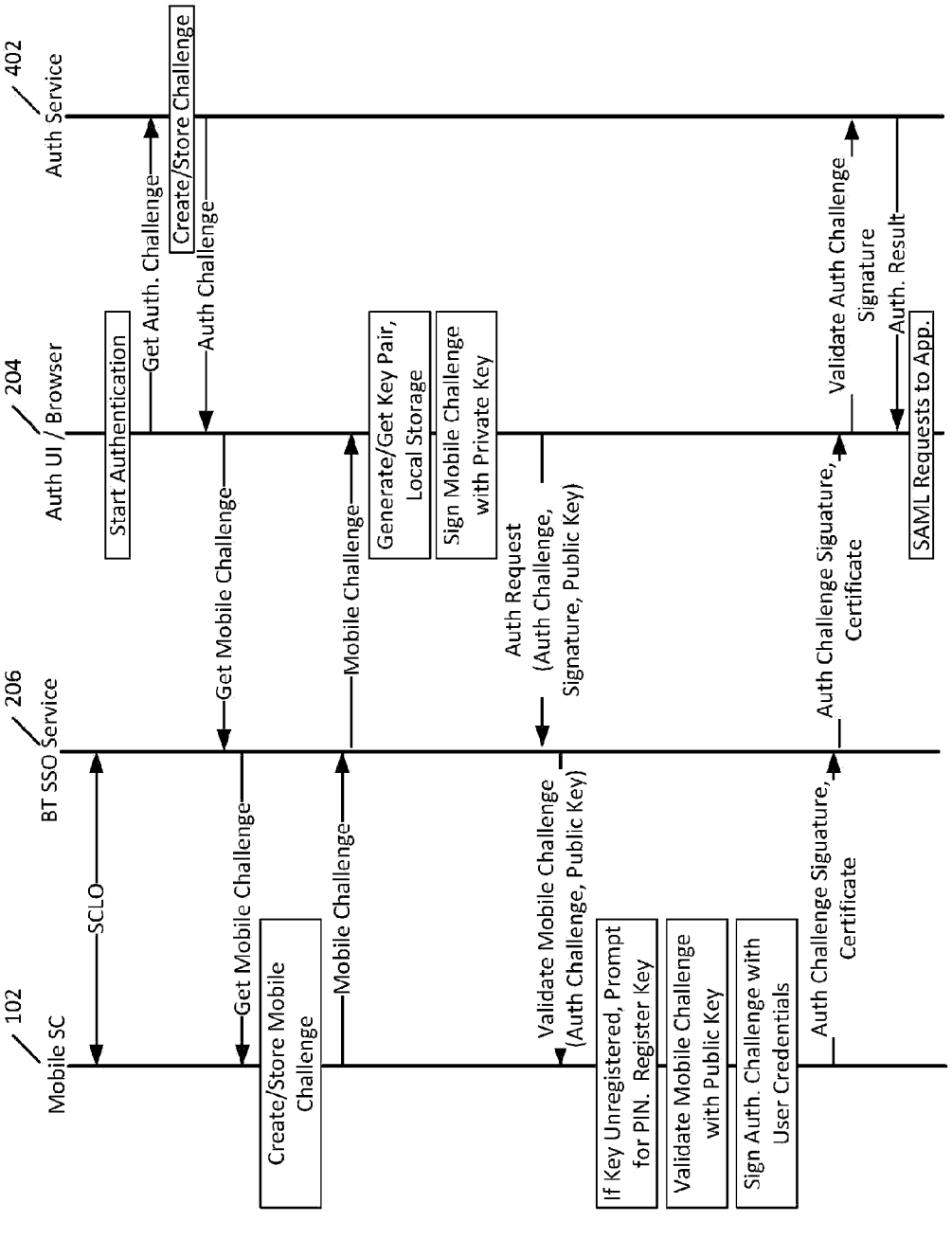
402
Auth Service
204
Auth UI / Browser
206
BT SSO Service
102
Mobile SC
Start Authentication
Get Auth. Challenge
Create/Store Challenge
Auth Challenge
Get Mobile Challenge
Mobile Challenge
Generate/Get Key Pair, Local Storage
Sign Mobile Challenge with Private Key
Auth Request (Auth Challenge, Signature, Public Key)
Validate Auth Challenge Signature
Auth. Result
SAML Requests to App.
SCLO
Get Mobile Challenge
Mobile Challenge
Validate Mobile Challenge (Auth Challenge, Public Key)
Auth Challenge Siguature, Certificate
Create/Store Mobile Challenge
If Key Unregistered, Prompt for PIN. Register Key
Validate Mobile Challenge with Public Key
Sign Auth. Challenge with User Credentials
Auth Challenge Siguature, Certificate
700

FIG. 5

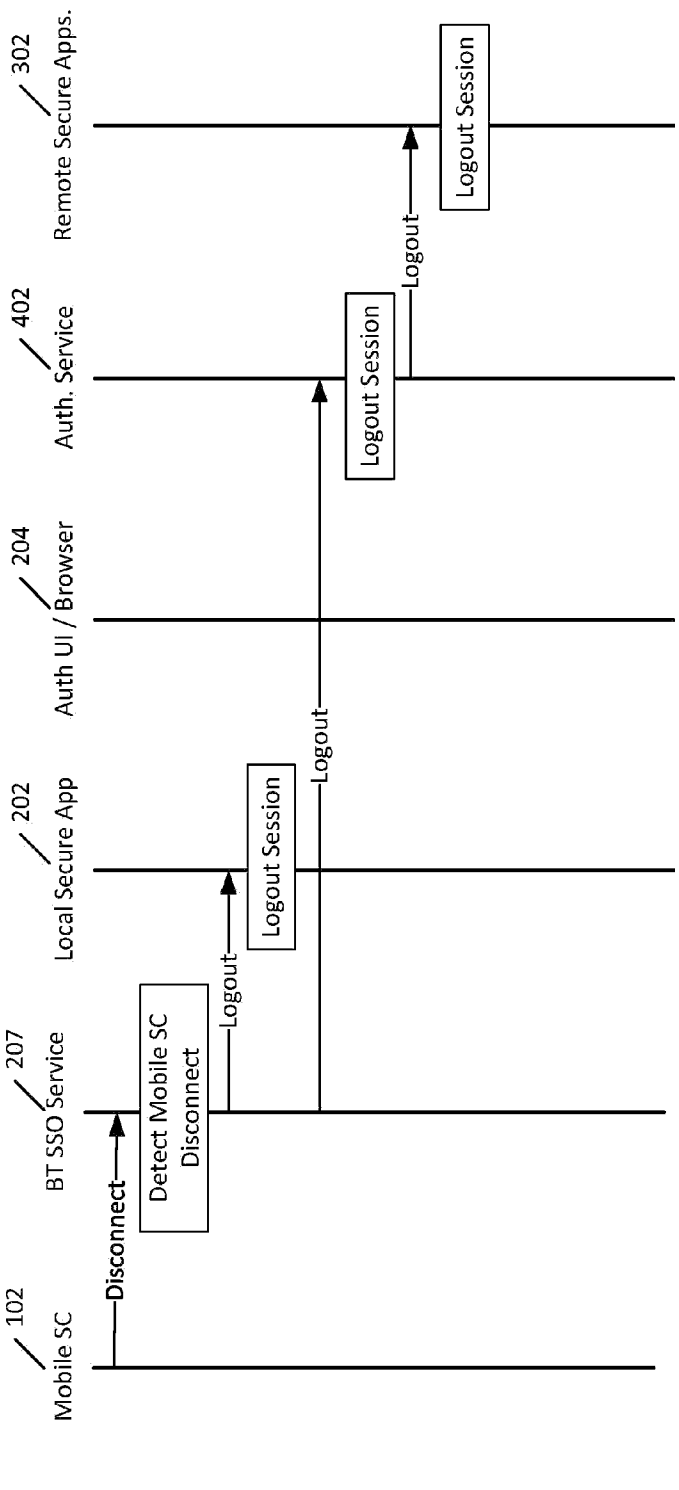
102
Mobile SC
207
BT SSO Service
202
Local Secure App
204
Auth UI / Browser
402
Auth. Service
302
Remote Secure Apps.
Disconnect
Detect Mobile SC Disconnect
Logout
Logout Session
Logout
Logout Session
Logout
Logout Session
800

FIG. 6