(12) STANDARD PATENT (11) Application No. **AU 2013274350 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Systems and methods for accessing a virtual desktop

(51) International Patent Classification(s)
G06F 21/41 (2013.01) ***H04L 29/06*** (2006.01)
G06F 21/33 (2013.01)

(21) Application No: **2013274350** (22) Date of Filing: **2013.06.11**

(87) WIPO No: **WO13/188455**

(30) Priority Data

(31) Number	(32) Date	(33) Country
13/524,412	**2012.06.15**	**US**

(43) Publication Date: **2013.12.19**
(44) Accepted Journal Date: **2015.09.10**

(71) Applicant(s)
VMware, Inc.

(72) Inventor(s)
Larsson, Per Olov

(74) Agent / Attorney
FB Rice, Level 14 90 Collins Street, Melbourne, VIC, 3000

(56) Related Art
US 2012/011578 A1 (HINTON et al.) 12 January 2012

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 December 2013 (19.12.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/188455 A1

(51) International Patent Classification:
G06F 21/41 (2013.01) *H04L 29/06* (2006.01)
G06F 21/33 (2013.01)

(21) International Application Number:
PCT/US2013/045253

(22) International Filing Date:
11 June 2013 (11.06.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/524,412 15 June 2012 (15.06.2012) US

(71) Applicant: **VMWARE, INC.** [US/US]; 3401 Hillview Avenue, Palo Alto, CA 94304 (US).

(72) Inventor: **LARSSON, Per Olov**; Blue Fin Building (12th Floor), 110 Southwark Street, London SE1 OTA (GB).

(74) Agents: **SMITH, Darryl A.** et al.; VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, 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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: SYSTEMS AND METHODS FOR ACCESSING A VIRTUAL DESKTOP

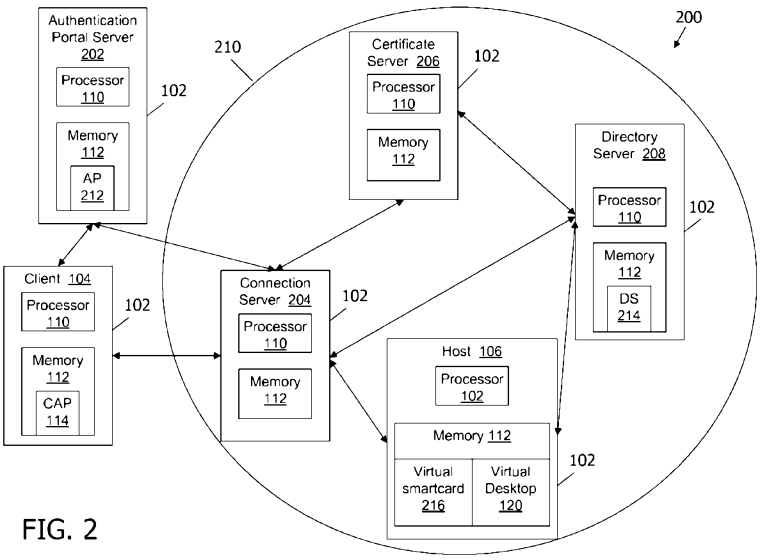

FIG. 2

(57) Abstract: Methods, computer-readable storage medium, and systems described herein facilitate enabling access to a virtual desktop of a host computing device. An authentication system receives one of an authentication token and a reference to the authentication token, wherein the authentication token is indicative of whether a user successfully logged in to an authentication portal using a client computing device. The authentication system generates a private key, a digital certificate, and a personal identification number (PIN) for the user in response to receiving the one of the authentication token and the reference to the authentication token. The private key, the digital certificate, and the PIN are stored in a virtual smartcard, and the client computing device is authorized to log into a virtual desktop using the virtual smartcard.

WO 2013/188455 A1

SYSTEMS AND METHODS FOR ACCESSING A VIRTUAL DESKTOP

BACKGROUND

[0001] Virtual machines (VMs) may be executed by a group, or "cluster," of host computing devices. Each VM provides an abstraction of physical computing resources, such as a processor and memory, of the host executing the VM. The guest operating system and guest software applications executing within a VM may function in a manner consistent with how they would function when executing directly on physical resources.

[0002] A VM may provide a virtual desktop that is accessible by one or more remote users through a network. A virtual desktop is a virtual machine configured with a guest operating system and productivity software intended for interaction with an end user. Typically, each virtual desktop is configured as a standard physical desktop computer system that, along with productivity applications such as word processors, spreadsheets, email, etc., provide a rich user interface for interaction with a particular user – the user for whom the desktop is configured and to whom the desktop is assigned.

[0002a] Any discussion of documents, acts, materials, devices, articles or the like which has been included in the present specification is not to be taken as an admission that any or all of these matters form part of the prior art base or were common general knowledge in the field relevant to the present disclosure as it existed before the priority date of each claim of this application.

[0002b] Throughout this specification the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated element, integer or step, or group of elements, integers or steps, but not the exclusion of any other element, integer or step, or group of elements, integers or steps.

[0003] As with physical desktops, each virtual desktop may require a user to supply login credentials to enable the user to access the virtual desktop, however with virtual desktops, the user may be accessing their system remotely requiring the user to supply login credentials using a client computing device. As a plurality of virtual desktops may be accessible to the user, the user may be required to maintain different access credentials (e.g., a username and password) for each virtual desktop and may be required to enter the access credentials for each virtual desktop that the user desires to access. In addition, if the user's password expires for one or more virtual desktops, the user may not be able to log into the virtual desktops until the password is changed.

SUMMARY

[0004] An authentication system is provided comprising:

a plurality of access-protected network resources, each of the access-protected network resources having respective access permissions;

a first computing device comprising a first processor configured to:

receive an access request and access credentials from a first user;

determine that the access credentials are valid; and

in response to determining that the access credentials are valid, authenticate the first user and generate an authentication token for the first user; and

a second computing device comprising a second processor configured to:

receive a request from the first user to access a first access-protected network resource of the plurality of access-protected network resources;

receive one of the authentication token for the first user or a reference to the authentication token;

determine that the first user has permission to access the first access-protected network resource;

generate smartcard credentials for the first user, wherein the smartcard credentials comprise a private key and a digital certificate with a public key for the first user;

store the smartcard credentials in a virtual smartcard;

associate the virtual smartcard with the first access-protected network resource to allow the first user to access the first access-protected network resource using the smartcard credentials without entering additional access credentials;

receive a request from the first user to access a second access-protected network resource of the plurality of access-protected network resources, the second access-protected network resource having different access permissions from the first access-protected network resource;

determine that the first user has permission to access the second access-protected network resource from one of the authentication token or a reference to the authentication token; and

associate the virtual smartcard with the second access-protected network resource to allow the first user to access the second access-protected network resource using the smartcard credentials without entering additional access credentials, wherein:

the plurality of access-protected network resources, the first computing device, and the second computing device are included within a domain.

[0004a] A non-transitory computer-readable storage medium is provided having computer-executable instructions stored thereon that, when executed by one or more computing devices, cause the computing devices to perform operations comprising:

receiving a request from a first user to access a first access-protected virtual desktop of a plurality of access-protected virtual desktops;

receiving one of an authentication token or a reference to the authentication token, wherein the authentication token indicates that the first user successfully logged in to an authentication portal by submitting access credentials to the authentication portal;

determining that the first user has permission to access the first access-protected virtual desktop;

generating smartcard credentials for the first user, wherein the smartcard credentials comprise a private key, a digital certificate, and a personal identification number (PIN) for the first user;

storing the smartcard credentials in a virtual smartcard;

authorizing the client computing device to log into the first access-protected virtual desktop using the smartcard credentials stored in the virtual smartcard, without entering additional access credentials;

receive a request from the first user to access a second access-protected network resource of the plurality of access-protected network resources, the second access-protected network resource having different access permissions from the first access-protected network resource;

determine that the first user has permission to access the second access-protected network resource from one of the authentication token or a reference to the authentication token; and

associate the virtual smartcard with the second access-protected network resource to allow the first user to access the second access-protected network resource using the smartcard credentials without entering additional access credentials, wherein:

the plurality of access-protected network resources and the one or more devices are included within a domain.

[0004b] A method is provided of authorizing a first user to access access-protected virtual desktops, the method comprising:

receiving, by a first computing device, a request from the first user to access a first access-protected virtual desktop of a plurality of access-protected virtual desktops;

receiving, by the first computing device, one of an authentication token or a reference to the authentication token, wherein the authentication token indicates that the first user successfully logged in to an authentication portal by submitting access credentials to the authentication portal;

determining that the first user has permission to access the first access-protected virtual desktop;

generating smartcard credentials for the first user, wherein the smartcard credentials comprise a private key, a digital certificate, and a personal identification number (PIN) for the first user;

storing the smartcard credentials in a virtual smartcard; and

associating the virtual smartcard with the first access-protected virtual desktop to allow the first user to log in to the first access-protected virtual desktop using the smartcard credentials without entering additional access credentials;

receiving a request from the first user to access a second access-protected network resource of the plurality of access-protected network resources, the second access-protected network resource having different access permissions from the first access-protected network resource;

determining that the first user has permission to access the second access protected network resource from one of the authentication token or a reference to the authentication token; and

associating the virtual smartcard with the second access-protected network resource to allow the first user to access the second access-protected network resource using the smartcard credentials without entering additional access credentials, wherein:

the plurality of access-protected network resources and the first computing device are included within a domain.

[0004c] Methods, computer-readable storage medium, and systems described herein facilitate enabling access to a virtual desktop of a host computing device. An authentication system receives one of an authentication token and a reference to the

authentication token, wherein the authentication token is indicative of whether a user successfully logged into an authentication portal using a client computing device. The authentication system generates a private key, a digital certificate, and a personal identification number (PIN) for the user in response to receiving either the authentication token or the reference to the authentication token. The private key, the digital certificate, and the PIN are stored in a virtual smartcard, and the client computing device is authorized to log into a virtual desktop using the virtual smartcard.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] FIG. 1 is a block diagram of an exemplary system for accessing a virtual desktop of a computing device.

[0006] FIG. 2 is a block diagram of an exemplary authentication system that includes a plurality of computing devices.

[0007] FIG. 3 is a flowchart of an exemplary method for accessing a virtual desktop that may be used with the authentication system shown in FIG. 2.

DETAILED DESCRIPTION

[0008] FIG. 1 is a block diagram of an exemplary system 100 for accessing a network resource, such as a remote or virtual desktop. System 100 includes a plurality of computing devices 102, such as a client computing device 104 (hereinafter referred to as "client 104") and a host computing device 106 (hereinafter referred to as "host 106") communicatively coupled to client 104 by a network 108. A user employs client 104 to access resources of host 106, as described more fully herein.

[0009] Each computing device 102 includes a processor 110 for executing instructions. Computing devices 102 may be heterogeneous and diverse. Client 104 may be, for example, a stateless or otherwise thin client, may be a tablet or mobile device, or an application running on a traditional computer system. Computer-executable instructions are stored in a memory 112 for performing one or more of the operations described herein. Memory 112 is any device allowing information, such as executable instructions, configuration options, and/or other data, to be stored and retrieved. For example, memory 112 includes one or more computer-readable storage media, such as one or more random

access memory (RAM) modules, flash memory modules, hard disks, solid state disks, and/or optical disks.

[0010] Client 104 includes processor 110 and memory 112. In addition, client 104 includes a client access program 114 that is stored within memory 112 as a plurality of computer-readable instructions that are executable by processor 110. Client access program 114 is executed to enable the user to connect to host 106 and to access the resources of host 106. Client 104 may be a desktop computer, a server, a smart phone, a tablet computer, a thin client, or any other computing device that enables system 100 to function as described herein.

[0011] Host 106 includes processor 110 and memory 112. In addition, host 106 includes a virtualization software layer, such as a hypervisor 116, that is installed on a hardware platform of host 106, including processor 110 and memory 112. The virtualization software layer may supports a plurality of virtual machine execution spaces within each of which a virtual machines (VMs) 118 may be concurrently instantiated and executed. Hypervisor 116 maps physical resources of host 106 to virtual resources of each VM 118 and may enable each VM 118 to have dedicated execution space and resources.

[0012] In addition, VMs 118 may be configured as, or may include, virtual desktops 120 that each includes a guest operating system 122 and a plurality of guest applications 124. Users may "log in" to (i.e., be authenticated by) virtual desktop 120 and/or host 106 to access the resources of desktop 120, such as applications 124 and operating system 122. A communication agent 126 may be included within virtual desktop 120 to facilitate authentication and communication between client 104 and virtual desktop 120.

[0013] FIG. 2 is a block diagram of an exemplary authentication system 200 that may be used to enable access to a virtual desktop 120 by a client 104. Authentication system 200 includes a plurality of computing devices 102, such as client 104, one or more hosts 106, an authentication portal server 202, a connection server 204, a certificate server 206, and a directory server 208. In an embodiment, connection server 204, certificate server 206, host 106, and directory server 208 are grouped within a domain 210. Although represented as being on corresponding physical devices 102, it should be recognized that the functionality of directory server 204, certificate server 206, and connection server 204 may be combined into a single server application or multiple server applications on a single

physical system, or may reside on disparate virtual machines executing at arbitrary locations, on the same physical system or multiple different physical systems, or any combination of the above, within or accessible from, domain 210.

[0014] Computing devices 102 within domain 210 may require a user to undergo separate authentication processes to enable access to computing devices 102. Authentication system 200 facilitates enabling a single sign-on (SSO) of client 104 (i.e., the user of client 104) to computing devices 102 of domain 210 such that the user of client 104 may only be required to enter authentication credentials, such as a username and password, once to enable authentication and access computing devices 102 of domain 210.

[0015] Authentication portal server 202 is communicatively coupled to client 104 and to connection server 204. Authentication portal server 202 includes an authentication portal ("AP") 212 that is embodied as a plurality of computer-executable instructions stored within memory 112 and that is executed by processor 110 to perform the functions described herein. Authentication portal 212 operates as a trusted authority and facilitates establishing a level of trust within domain 210 for the user when the user is authenticated by authentication portal 212. In an embodiment, authentication portal 212 includes a VMware Horizon Program Manager program suite that is commercially available from VMware, Inc., of Palo Alto, California. Alternatively, authentication portal 212 may be any other portal or gateway that enables authentication system 200 to function as described herein.

[0016] Connection server 204 is communicatively coupled to client 104, authentication portal server 202, certificate server 206, host 106, and directory server 208. Connection server 204 facilitates the authentication of the user within domain 210, and specifically the authentication of the user with one or more virtual desktops 120, based on the trust level of the user that is established by authentication portal 212.

[0017] Certificate server 206 is communicatively coupled to connection server 204 and to directory server 208. Certificate server 206 generates and validates cryptographic digital certificates for use in authenticating the user to computing devices 102 within domain 210.

[0018] Directory server 208 is communicatively coupled to certificate server 206, connection server 204, and host 106. Directory server 208 includes a directory service

("DS") 214 that is embodied as a plurality of computer-executable instructions stored within memory 112 and that is executed by processor 110 to perform the functions described herein. In an embodiment, directory service 214 configures and manages user accounts and permissions within domain 210.

[0019] During operation, a user who desires to access a virtual desktop 120 first logs into authentication portal 212 by transmitting (via client 104) access credentials, such as a username and a password, to authentication portal 212. Authentication portal 212 authenticates the user by determining whether the access credentials are valid to enable access to portal 212. If the access credentials are valid, authentication portal 212 generates an authentication token indicative of the successful authentication. In an embodiment, the authentication token is a security assertion markup language (SAML) assertion that the user was authenticated by authentication portal 212.

[0020] The user, through client 104, requests access to virtual desktop 120 by transmitting a connection request to connection server 204. Connection server 204 verifies the user's access permissions with directory service 214, and uses the authentication token to determine whether the user is trusted. If the user is trusted, connection server 204 generates a private key, a digital certificate, and a personal identification number (PIN) for the user. In an embodiment, the private key, the digital certificate, and the PIN are "one-off" credentials that are only valid for a single connection session with the user. In addition, the PIN is a random number that is associated with the digital certificate, i.e., that is associated with an ability to perform cryptographic operations using the private key associated with the digital certificate. Alternatively, the PIN may include any other alphanumeric character, symbol, and/or entry that enables authentication system 200 to function as described herein. In an embodiment, connection server 204 stores the private key, the digital certificate, and the PIN in a virtual smartcard 216.

[0021] Virtual smartcard 216 is stored within host 106 and is communicatively coupled to, or stored within, the virtual desktop 120 that the user is requesting access to. Virtual smartcard 216 is a software-based representation of a physical smartcard or authentication device that stores credentials, such as a private key, a digital certificate, and optionally, a PIN. The credentials are used to authenticate the user associated with virtual smartcard 216 and to enable the user to access resources within domain 210 without having to enter a username and a password.

[0022] Client 104 connects to virtual desktop 120 and uses virtual smartcard 216 in lieu of providing access credentials, such as a username and password, to virtual desktop 120. Virtual desktop 120 authenticates the user via virtual smartcard 216 (e.g., using the private key, the digital certificate, and the PIN) with directory service 214 and certificate server 206. If the user is authenticated, the user is granted access to virtual desktop 120.

[0023] It should be understood that the user may access a plurality of virtual desktops 120, each having different access credential requirements, using virtual smartcard 216 and authentication system 200 while only being required to enter access credentials (e.g., the username and password) once at authentication portal 212. Accordingly, authentication system 200 enables users to access virtual desktops 120 and/or other resources within domain 210 even if the user does not know a password to virtual desktop 120 and/or the other resources. It should be understood that authentication system 200 may be used to enable a user to access resources other than virtual desktops, such as one or more physical computing devices 102, session-instances of one or more terminal servers, and/or applications executing on one or more computing devices 102, such as desktop computers and/or servers, while only being required to enter access credentials once at authentication portal 212.

[0024] FIG. 3 is a flowchart of an exemplary method 300 of accessing a virtual desktop of a host computing device ("host") from a client computing device ("client"). Method 300 may be used with system 100 (shown in FIG. 1) and/or authentication system 200 (shown in FIG. 2). Method 300 is embodied within a plurality of computer-executable instructions stored in one or more memories, such as one or more computer-readable storage mediums. The instructions are executed by one or more processors to perform the functions described herein.

[0025] Method 300 is executed or performed by an authentication system to enable access from a user, via the client, to an access-protected virtual desktop within a host. In addition, method 300 enables single sign-on access to the virtual desktop, and to other access-protected virtual desktops and/or resources of the authentication system, during a connection session of the user.

[0026] The connection session of the user is initiated when the user connects to an authentication portal. Method 300 includes authenticating 302 the user at the authentication portal using access credentials supplied by the user via the client. The access

credentials include, for example, a username and a password for the authentication portal. If the authentication portal determines that the access credentials are valid to enable access to the authentication portal, the portal displays 304 a list of virtual desktops that are accessible to the user based on user account settings and/or permissions, for example.

[0027] The authentication portal receives 306 a selection, from the client, of a virtual desktop that the user desires to access. A client access program may be executed within the client to facilitate communication and authentication to the virtual desktop. The authentication portal generates 308 an authentication token indicative of the successful authentication of the user and transmits 310 the authentication token to the client (e.g., to the client access program). In an embodiment, the authentication token is a SAML assertion that the user was authenticated by the authentication portal.

[0028] A connection server within the authentication system receives 312 a request (i.e., a connection request) from the client to connect to the selected virtual desktop. The connection request includes the authentication token, or a reference to the authentication token. The connection server verifies 314 the authentication token by transmitting the token (or reference) to the authentication portal. If the authentication token is valid, the connection server receives a confirmation of the token from the authentication portal. The confirmation verifies that the user is trusted by the authentication portal, and the connection server therefore trusts the user as well.

[0029] The connection server verifies 316 access permissions for the user, for example, by querying a directory service that contains user account permissions. If the user has sufficient permissions to access the virtual desktop, the connection server generates 318 credentials for a virtual smartcard. The virtual smartcard is used to facilitate SSO access to computing devices and/or virtual desktops that are otherwise access-restricted within a domain. The credentials for the virtual smartcard (also referred to as "smartcard credentials") include a private key, a digital certificate, and a personal identification number (PIN) for the user. The connection server stores 320 the smartcard credentials in the virtual smartcard, and associates the virtual smartcard with the virtual desktop that the user is attempting to connect to. For example, the virtual smartcard is stored within the host computing device of the virtual desktop and is communicatively coupled to the virtual desktop. Alternatively, the virtual smartcard is stored within the virtual desktop.

[0030] The connection server authorizes 322 the user's request to connect to the virtual desktop (i.e., the connection request received 312 above) to enable the user to send, via the client, a connection request to the virtual desktop. The virtual desktop receives 324 the connection request from the client. The connection request uses the smartcard credentials, rather than providing a username and password, to obtain access to the virtual desktop.

[0031] The virtual desktop authenticates 326 the user via the virtual smartcard credentials. As part of the authentication process, the virtual smartcard credentials are presented 328 to the directory service to log the user into the domain in which the virtual desktop resides. The virtual smartcard credentials are validated 330 by the directory service and the user logs into the domain. The virtual desktop receives 332 a token from the directory service that is representative of the identity and/or successful login of the user into the domain. The user is enabled 334 to access the virtual desktop and/or the resources contained therein. It should be recognized that the client and/or the authentication system may use the virtual smartcard to log into other virtual desktops in the domain without entering a username or a password to the virtual desktops.

[0032] The various embodiments described herein may employ various computer-implemented operations involving data stored in computer systems. For example, these operations may require physical manipulation of physical quantities--usually, though not necessarily, these quantities may take the form of electrical or magnetic signals, where they or representations of them are capable of being stored, transferred, combined, compared, or otherwise manipulated. Further, such manipulations are often referred to in terms, such as producing, identifying, determining, or comparing. Any operations described herein that form part of one or more embodiments of the invention may be useful machine operations. In addition, one or more embodiments of the invention also relate to a device or an apparatus for performing these operations. The apparatus may be specially constructed for specific required purposes, or it may be a general purpose computer selectively activated or configured by a computer program stored in the computer. In particular, various general purpose machines may be used with computer programs written in accordance with the teachings herein, or it may be more convenient to construct a more specialized apparatus to perform the required operations.

[0033] The various embodiments described herein may be practiced with other computer system configurations including hand-held devices, microprocessor systems, microprocessor-based or programmable consumer electronics, minicomputers, mainframe computers, and the like.

[0034] One or more embodiments of the present invention may be implemented as one or more computer programs or as one or more computer program modules embodied in one or more computer readable media. The term computer readable medium refers to any data storage device that can store data which can thereafter be input to a computer system--computer readable media may be based on any existing or subsequently developed technology for embodying computer programs in a manner that enables them to be read by a computer. Examples of a computer readable medium include a hard drive, network attached storage (NAS), read-only memory, random-access memory (e.g., a flash memory device), a CD (Compact Discs) --CD-ROM, a CD-R, or a CD-RW, a DVD (Digital Versatile Disc), a magnetic tape, and other optical and non-optical data storage devices. The computer readable medium can also be distributed over a network coupled computer system so that the computer readable code is stored and executed in a distributed fashion.

[0035] Although one or more embodiments of the present invention have been described in some detail for clarity of understanding, it will be apparent that certain changes and modifications may be made within the scope of the claims. Accordingly, the described embodiments are to be considered as illustrative and not restrictive, and the scope of the claims is not to be limited to details given herein, but may be modified within the scope and equivalents of the claims. In the claims, elements and/or steps do not imply any particular order of operation, unless explicitly stated in the claims.

[0036] In addition, while described virtualization methods have generally assumed that virtual machines present interfaces consistent with a particular hardware system, persons of ordinary skill in the art will recognize that the methods described may be used in conjunction with virtualizations that do not correspond directly to any particular hardware system. Virtualization systems in accordance with the various embodiments, implemented as hosted embodiments, non-hosted embodiments or as embodiments that tend to blur distinctions between the two, are all envisioned. Furthermore, various virtualization operations may be wholly or partially implemented in hardware, or implemented with traditional virtualization or paravirtualization techniques. Many variations, modifications,

additions, and improvements are possible, regardless the degree of virtualization. The virtualization software can therefore include components of a host, console, or guest operating system that performs virtualization functions. Plural instances may be provided for components, operations or structures described herein as a single instance. Finally, boundaries between various components, operations and data stores are somewhat arbitrary, and particular operations are illustrated in the context of specific illustrative configurations. Other allocations of functionality are envisioned and may fall within the scope of the invention(s). In general, structures and functionality presented as separate components in exemplary configurations may be implemented as a combined structure or component. Similarly, structures and functionality presented as a single component may be implemented as separate components. These and other variations, modifications, additions, and improvements may fall within the scope of the appended claims(s).

2013274350 20 Aug 2015

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. An authentication system comprising:

a plurality of access-protected network resources, each of the access-protected network resources having respective access permissions;

a first computing device comprising a first processor configured to:

receive an access request and access credentials from a first user;

determine that the access credentials are valid; and

in response to determining that the access credentials are valid, authenticate the first user and generate an authentication token for the first user; and

a second computing device comprising a second processor configured to:

receive a request from the first user to access a first access-protected network resource of the plurality of access-protected network resources;

receive one of the authentication token for the first user or a reference to the authentication token;

determine that the first user has permission to access the first access-protected network resource;

generate smartcard credentials for the first user, wherein the smartcard credentials comprise a private key and a digital certificate with a public key for the first user;

store the smartcard credentials in a virtual smartcard;

associate the virtual smartcard with the first access-protected network resource to allow the first user to access the first access-protected network resource using the smartcard credentials without entering additional access credentials;

receive a request from the first user to access a second access-protected network resource of the plurality of access-protected network resources, the second access-protected network resource having different access permissions from the first access-protected network resource;

determine that the first user has permission to access the second access-protected network resource from one of the authentication token or a reference to the authentication token; and

associate the virtual smartcard with the second access-protected network resource to allow the first user to access the second access-protected network resource using the smartcard credentials without entering additional access credentials, wherein:

the plurality of access-protected network resources, the first computing device, and the second computing device are included within a domain.

2. The authentication system of claim 1, wherein the authentication token includes a security assertion markup language (SAML) assertion that the first user was authenticated.

3. The authentication system of claim 1, further comprising a directory service, wherein determining that the first user has permission to access the first access-protected network resource comprises transmitting a request to the directory service to validate whether the first user has permission to access the access-protected network resource.

4. The authentication system of claim 1, wherein the first processor is further configured to transmit, to the second computing device, the authentication token or the reference to the authentication token.

5. The authentication system of claim 1, wherein the second processor is further configured to validate the authentication token with an authentication portal.

6. The authentication system of claim 1, wherein the system further comprises a directory service included within the domain.

7. The authentication system of claim 6, wherein the second computing device is further configured to log the first user into the directory service using the virtual smartcard.

8. A non-transitory computer-readable storage medium having computer-executable instructions stored thereon that, when executed by one or more computing devices, cause the computing devices to perform operations comprising:

receiving a request from a first user to access a first access-protected virtual desktop of a plurality of access-protected virtual desktops;

receiving one of an authentication token or a reference to the authentication token, wherein the authentication token indicates that the first user successfully logged in to an authentication portal by submitting access credentials to the authentication portal;

determining that the first user has permission to access the first access-protected virtual desktop;

generating smartcard credentials for the first user, wherein the smartcard credentials comprise a private key, a digital certificate, and a personal identification number (PIN) for the first user;

storing the smartcard credentials in a virtual smartcard;

authorizing the client computing device to log into the first access-protected virtual desktop using the smartcard credentials stored in the virtual smartcard, without entering additional access credentials;

receive a request from the first user to access a second access-protected network resource of the plurality of access-protected network resources, the second access-protected network resource having different access permissions from the first access-protected network resource;

determine that the first user has permission to access the second access-protected network resource from one of the authentication token or a reference to the authentication token; and

associate the virtual smartcard with the second access-protected network resource to allow the first user to access the second access-protected network resource using the smartcard credentials without entering additional access credentials, wherein:

the plurality of access-protected network resources and the one or more devices are included within a domain.

9. The computer-readable storage medium of claim 8, wherein the computer-executable instructions further cause the at least one processor to transmit a request to a directory service to determine whether the first user has permission to access the first access-protected virtual desktop.

10. The computer-readable storage medium of claim 9, wherein the computer-executable instructions further cause the at least one processor to log the first user into the directory service using the virtual smartcard.

11. The computer-readable storage medium of claim 8, wherein the computer-executable instructions further cause the at least one processor to transmit a login request to the authentication portal, wherein the login request includes the access credentials associated with the user.

12. The computer-readable storage medium of claim 11, wherein the computer-executable instructions further cause the at least one processor to receive the authentication token or the reference to the authentication token from the authentication portal in response to the login request.

13. A method of authorizing a first user to access access-protected virtual desktops, the method comprising:

receiving, by a first computing device, a request from the first user to access a first access-protected virtual desktop of a plurality of access-protected virtual desktops;

receiving, by the first computing device, one of an authentication token or a reference to the authentication token, wherein the authentication token indicates that the first user successfully logged in to an authentication portal by submitting access credentials to the authentication portal;

determining that the first user has permission to access the first access-protected virtual desktop;

generating smartcard credentials for the first user, wherein the smartcard credentials comprise a private key, a digital certificate, and a personal identification number (PIN) for the first user;

storing the smartcard credentials in a virtual smartcard; and

associating the virtual smartcard with the first access-protected virtual desktop to allow the first user to log in to the first access-protected virtual desktop using the smartcard credentials without entering additional access credentials;

receiving a request from the first user to access a second access-protected network resource of the plurality of access-protected network resources, the second access-protected network resource having different access permissions from the first access-protected network resource;

determining that the first user has permission to access the second access protected network resource from one of the authentication token or a reference to the authentication token; and

associating the virtual smartcard with the second access-protected network resource to allow the first user to access the second access-protected network resource using the smartcard credentials without entering additional access credentials, wherein:

the plurality of access-protected network resources and the first computing device are included within a domain.

14. The method of claim 13, wherein determining that the first user has permission to access the first access-protected virtual desktop further comprises transmitting a request to a directory service to validate whether the user has permission to access the first access-protected virtual desktop.

15. (The method of claim 14, further comprising transmitting, by a second computing device, the access credentials to the authentication portal.

16. The method of claim 15, further comprising receiving, by the second computing device, the authentication token or the reference to the authentication token from the authentication portal.

17. The method of claim 16, further comprising transmitting, from the second computing device to the first computing device, the authentication token and the reference to the authentication token.

18. The method of claim 13, further comprising logging the first user into a directory service using the virtual smartcard.

19. The method of claim 18, further comprising logging the user into the domain such that the first user is enabled to log into the plurality of access-protected virtual desktops within the domain using the smartcard credentials.

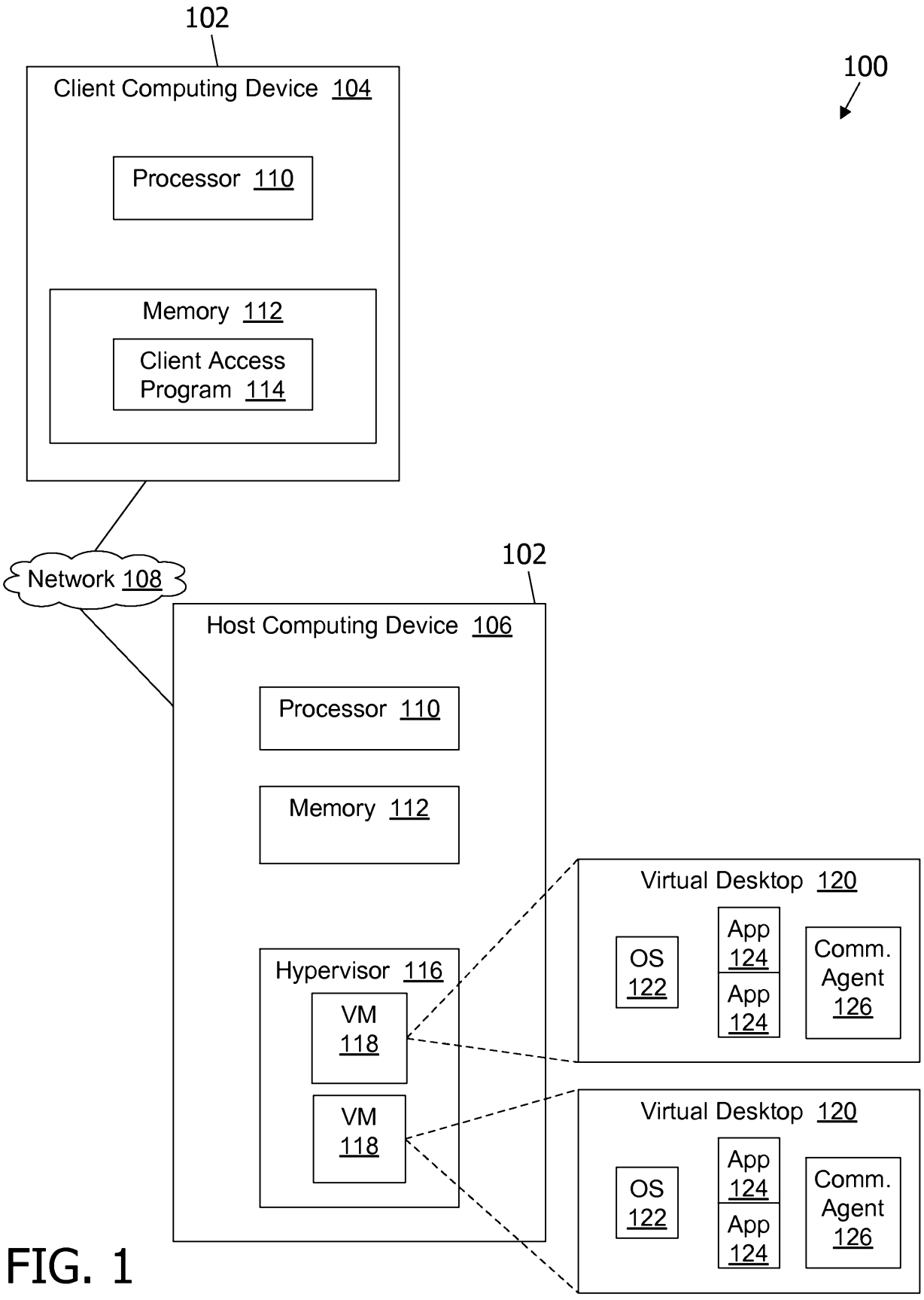
102
Client Computing Device 104
Processor 110
Memory 112
Client Access Program 114
100
Network 108
102
Host Computing Device 106
Processor 110
Memory 112
Hypervisor 116
VM 118
VM 118
Virtual Desktop 120
OS 122
App 124
App 124
Comm. Agent 126
Virtual Desktop 120
OS 122
App 124
App 124
Comm. Agent 126

FIG. 1

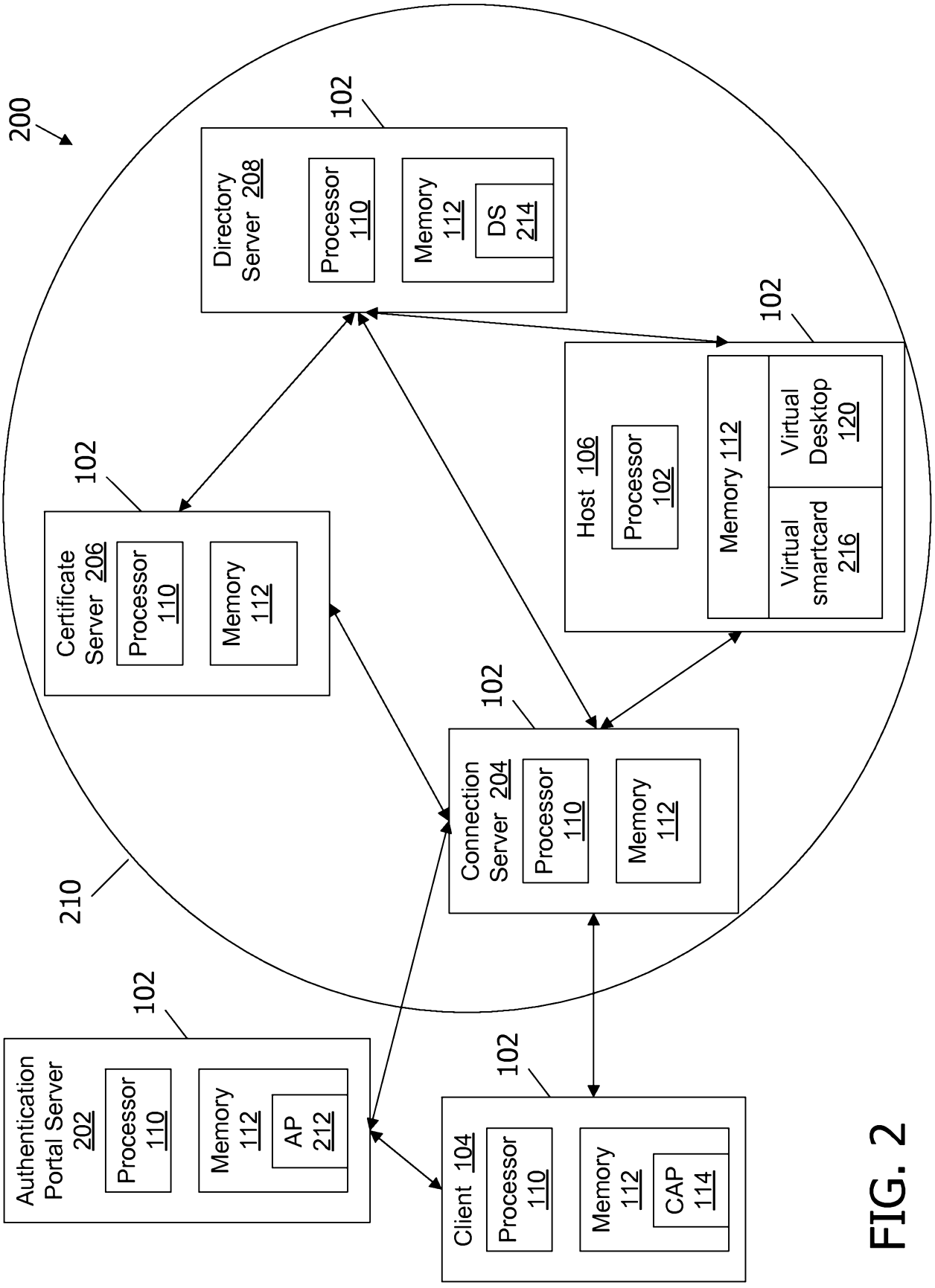
200
210
102
Directory Server 208
Processor 110
Memory 112
DS 214
102
Certificate Server 206
Processor 110
Memory 112
102
Host 106
Processor 102
Memory 112
Virtual Desktop 120
Virtual smartcard 216
102
Connection Server 204
Processor 110
Memory 112
102
Authentication Portal Server 202
Processor 110
Memory 112
AP 212
102
Client 104
Processor 110
Memory 112
CAP 114

FIG. 2

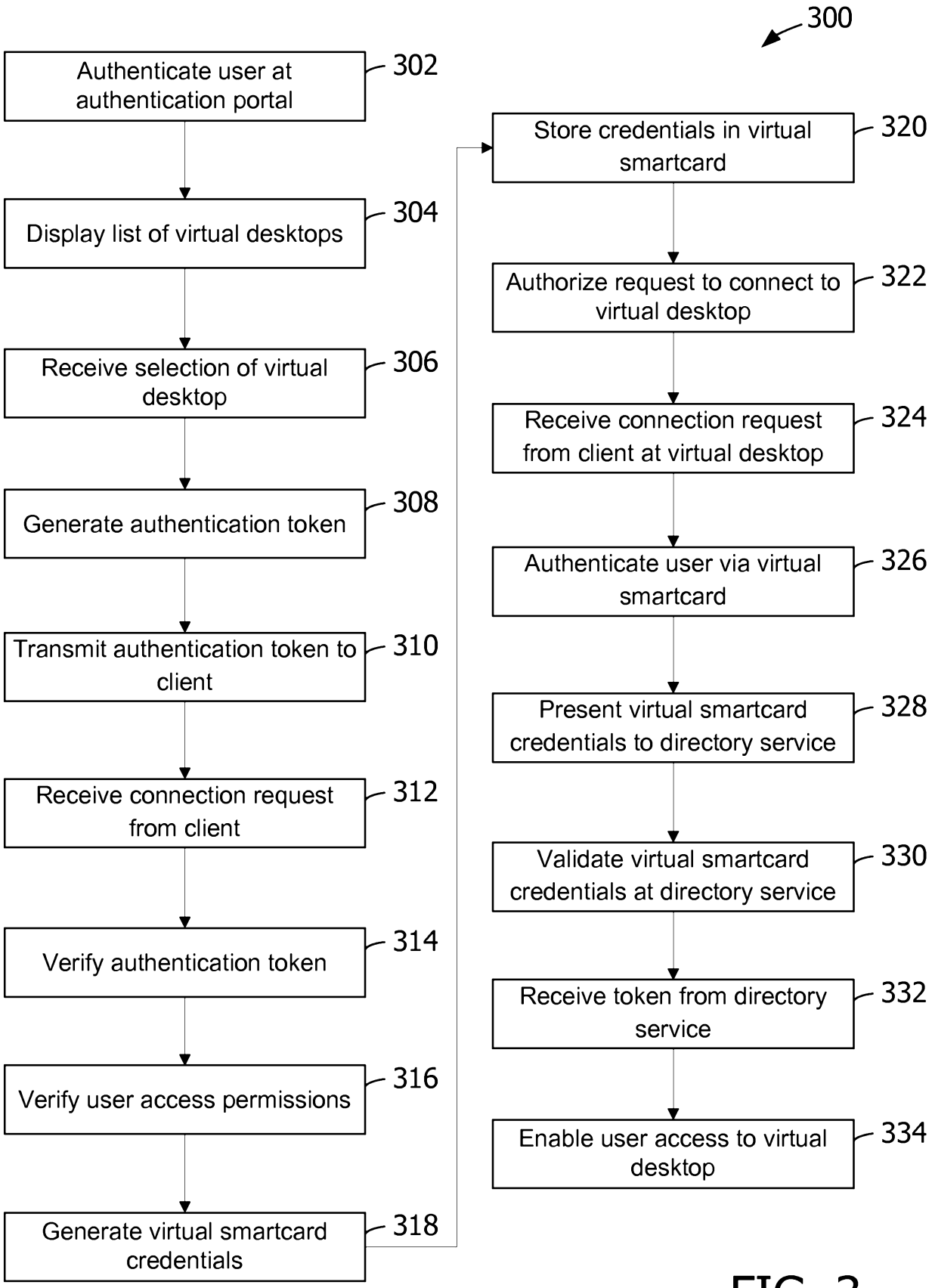
300
Authenticate user at authentication portal
302
Display list of virtual desktops
304
Receive selection of virtual desktop
306
Generate authentication token
308
Transmit authentication token to client
310
Receive connection request from client
312
Verify authentication token
314
Verify user access permissions
316
Generate virtual smartcard credentials
318
Store credentials in virtual smartcard
320
Authorize request to connect to virtual desktop
322
Receive connection request from client at virtual desktop
324
Authenticate user via virtual smartcard
326
Present virtual smartcard credentials to directory service
328
Validate virtual smartcard credentials at directory service
330
Receive token from directory service
332
Enable user access to virtual desktop
334

FIG. 3