(12) UK Patent (19) GB (11) 2518367 (13) B

(45) Date of B Publication 22.07.2020

(54) Title of the Invention: Authorized remote access to an operating system hosted by a virtual machine

(51) INT CL: ***G06F 9/455*** (2018.01) ***G06F 9/44*** (2018.01) ***G06F 21/30*** (2013.01)

(21) Application No: **1316561.8**

(22) Date of Filing: **18.09.2013**

(43) Date of A Publication **25.03.2015**

(56) Documents Cited:

US 20130031000 A1 **US 20130024920 A1**
US 20120239729 A1 **US 20120060153 A1**

(58) Field of Search:

As for published application 2518367 A viz:
INT CL **G06F**
Other: **Online: WPI, EPODOC, INSPEC, XPI3E, XPIEE, XPLNCS, XPMISC, XPESP, XPESP2, Springer, IP.COM, TDB, XPRD**
updated as appropriate

Additional Fields
Other: **None**

(72) Inventor(s):

Peter Jenkin
Anthony Blaise Hogg

(73) Proprietor(s):

International Business Machines Corporation
New Orchard Road, Armonk 10504, New York, United States of America

(74) Agent and/or Address for Service:

A A Thornton & Co
10 Old Bailey, LONDON, EC4M 7NG, United Kingdom

GB 2518367 B

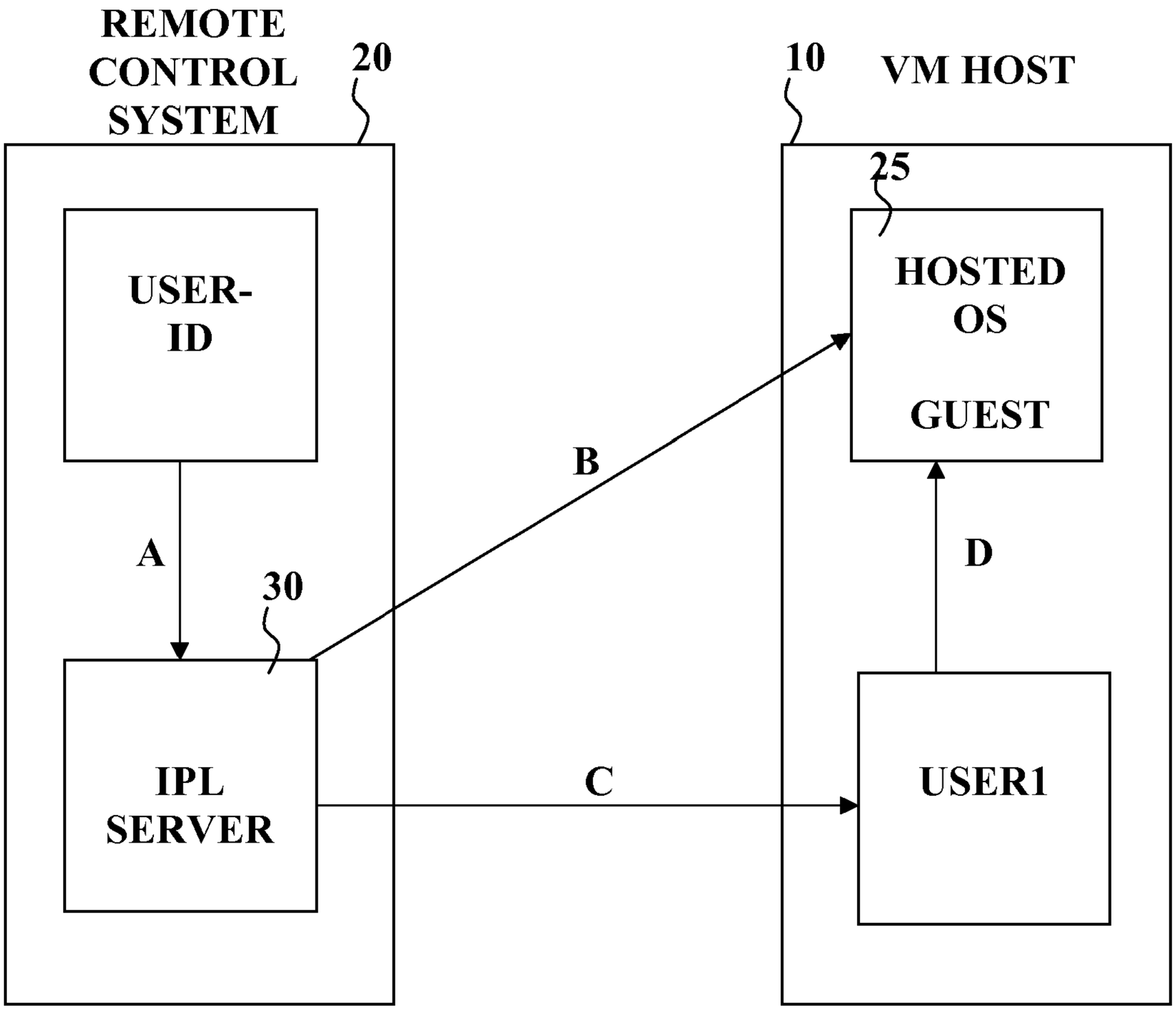
REMOTE CONTROL SYSTEM
20
USER-ID
A
30
IPL SERVER
B
C
10
VM HOST
25
HOSTED OS
GUEST
D
USER1

FIG. 1

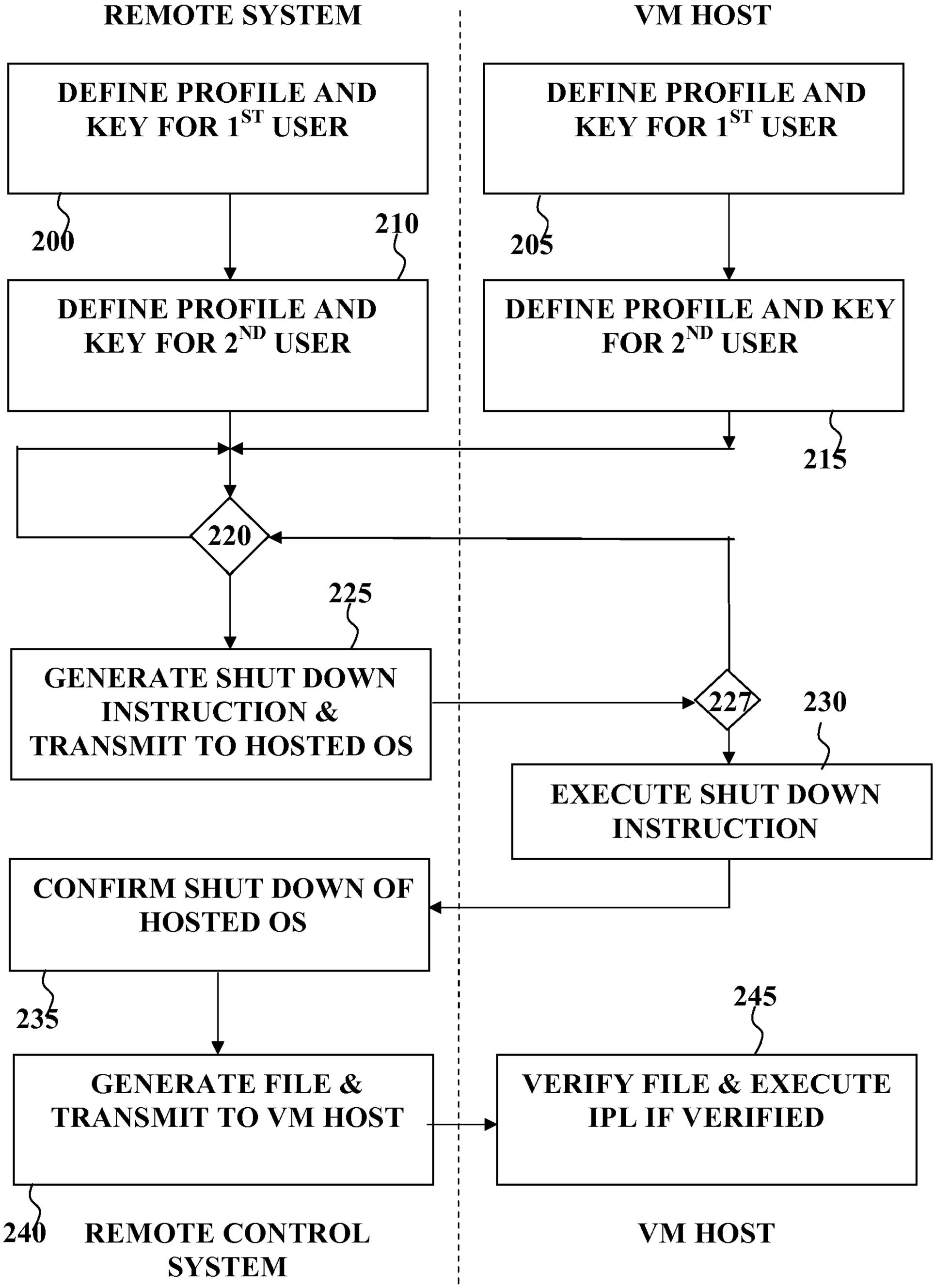
REMOTE SYSTEM
VM HOST
DEFINE PROFILE AND KEY FOR 1ST USER
DEFINE PROFILE AND KEY FOR 1ST USER
200
210
205
DEFINE PROFILE AND KEY FOR 2ND USER
DEFINE PROFILE AND KEY FOR 2ND USER
215
220
225
GENERATE SHUT DOWN INSTRUCTION & TRANSMIT TO HOSTED OS
227
230
EXECUTE SHUT DOWN INSTRUCTION
CONFIRM SHUT DOWN OF HOSTED OS
235
245
GENERATE FILE & TRANSMIT TO VM HOST
VERIFY FILE & EXECUTE IPL IF VERIFIED
240
REMOTE CONTROL SYSTEM
VM HOST

FIG. 2

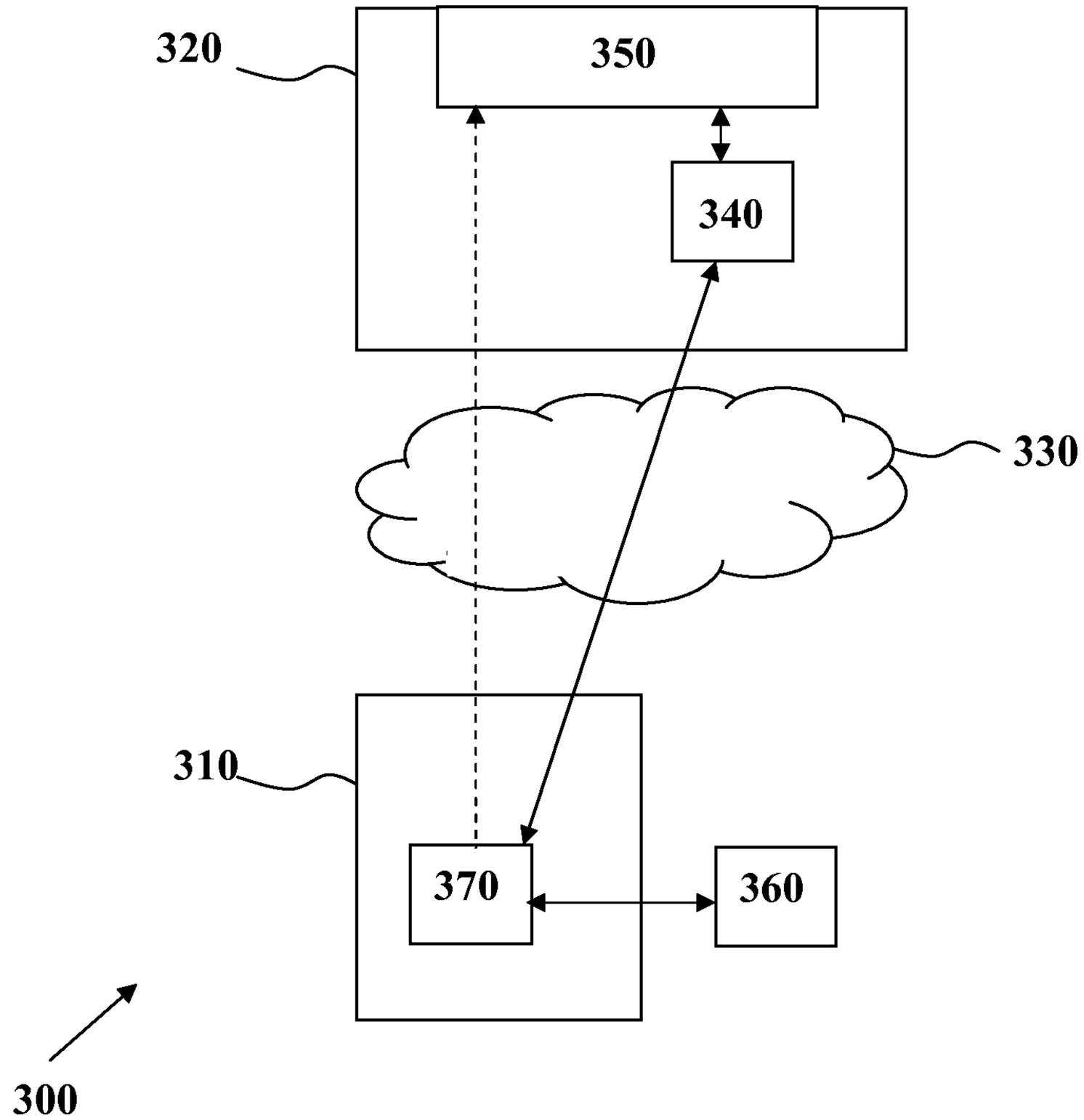

FIG. 3

AUTHORIZED REMOTE ACCESS TO AN OPERATING SYSTEM HOSTED BY A VIRTUAL MACHINE

FIELD OF THE INVENTION

[0001] This invention relates to the field of providing remote access to computer systems and more particularly to providing authorized remote access to an operating system hosted by a virtual machine.

BACKGROUND

[0002] Remote access computing is widely known in the field of computing. Typically, a remote access computing environment provides an operating system (OS) which runs on server hardware. A remote access program is implemented on the server which is accessible to users of the remote access program via a network.

[0003] Typically, the server runs a Virtual Machine (VM) which hosts an operating system supporting multiple guest systems, each capable of supporting multiple users in a unique environment. A VM is a software facility that allows one physical processor to be configured with multiple "virtual" processors or machine. Each VM normally runs independently of every other VM and may run any operating system and software.

[0004] Each remote access participant is typically provided with a dedicated guest OS, which appears to the user as a server running a native operating system. The guest OS will Initial Program Load (IPL) automatically when a VM user logs on and issues a command to start the process. Thus, before utilising a guest OS, a user must first access the server and initialise (i.e. IPL) the guest OS.

[0005] Techniques for securing such remote access have been sought, many of which are not appropriate or too expensive to implement.

BRIEF SUMMARY OF THE INVENTION

[0006] There is proposed a concept for providing authorised remote IPL in VM-hosted OSs. By employing a pass ticket, remote IPL requests for a VM-hosted (e.g. second level) OS may be authenticated so as to secure the control or use of the VM-hosted OS and/or prevent unauthorised remote access to the OS and its functionality. Using a resource access control facility (RACF), a passticket (such as a single use or 'use-once' password) or authentication key may be implemented which enables a remote IPL request to be checked and authenticated without requiring additional hardware or proprietary systems.

[0007] Thus, embodiments may be used to provide authorized remote access to an OS hosted by a VM. First and second authentication tokens may be generated at a client system and communicated to a server system providing the VM. The validity of the first and second authentication tokens may be verified at the server system. If the validity of the first authentication token is verified, the OS is shut-down. Then, if the validity of the second authentication token is verified, the OS is re-started.

[0008] According to an aspect of the invention, there is provided a method for performing an authorised IPL in a VM-hosted OS from a remote system.

[0009] According to an embodiment, there is provided a method for providing authorized remote access to an operating system hosted by a virtual machine, VM, the method comprising: on a remote system and on a VM-host, defining a first profile and first key for a first user of the hosted system and defining a second profile and second key for a second user of the hosted system; on receipt of a request for an initial program load at the remote system, creating a pass key for the second user, creating a shut-down instruction using the pass key for the second user, and sending the shut-down instruction to the VM-hosted system; on receipt of the shut-down instruction at the VM-hosted system, checking the shut-down instruction is valid by comparing the pass key for the second user with the second key and, if valid, executing the shut-down instruction on the VM-hosted system so as to shut-down the VM-hosted system; after the VM-hosted system is shut-down, creating a pass key for the first user and sending a record to the first user, the record containing the pass key for

the first user and an initial program load request; on receipt of the record, checking that the pass key for the first user is valid by comparing the pass key for the first user with the first key and, if valid, issuing a request for an initial program load to restart the VM-hosted system.

[00010] Prior to generating a second authentication token and an IPL instruction for the operating system, the OS may be monitored to determine when it is completely shut-down.

[00011] The shut-down instruction may further comprise at least one of: an identification of a user of the client system; and an identification of the operating system. Also, the IPL instruction may further comprise at least one of: an identification of a user of the client system; and an identification of the operating system. Accordingly, in an embodiment, at least one of: the first authentication token; and the second authentication token may be generated based on at least one of: the received request for an IPL; and authentication information provided by the client system or a user of the client system.

[00012] In an embodiment, at least one of: the first authentication token; and the second authentication token may comprise a one-time use pass key adapted to be rendered invalid after a single use. A single use of the one-time use pass key may comprise the process of verifying if the one-time passkey is valid, and the one-time passkey is valid may be rendered invalid irrespective of the outcome of the verification process. According to another aspect of the invention, there is provided a computer program product for providing authorized remote access to an OS hosted by a VM on server system.

[00013] According to yet another aspect of the invention, there is provided a client system for providing authorized remote access to an OS hosted by a VM of a server system.

[00014] According to a further aspect of the invention, there is provided a server system for providing authorized remote access to an operating system hosted by a VM of the server system.

BRIEF DESCRIPTION OF THE DRAWINGS

[00015] Preferred embodiments of the present invention will now be described, by way of example only, with reference to the following drawings in which:
Figure 1 is a block diagram illustrating an embodiment of the invention;
Figure 2 is a flow diagram of a method according to an embodiment of the invention; and
Figure 3 is a schematic block diagram of system according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[00016] It is proposed to define two user profiles, each with an associated authentication key. A remote IPL request may be firstly be authenticated against the second user profile and, if authenticated, the VM-hosted OS shut-down. Next, the remote IPL request may be secondly authenticated against the first user profile and, if authenticated, the VM-hosted OS may be re-started Authentication may employ one-time use passtickets, which are a form of single use key/password that can only be used a single time, thereby enabling secure authentication across a network (which may not be secure). In this way, remote IPL of the VM-hosted OS may be secured.

[00017] Referring to Figure 1, there is illustrated an embodiment of the invention. There is provided a concept for performing an authorised IPL in an OS of a VM host 10 from a remote system 20.

[00018] On the remote system 20, a first profile and first key is defined for a first user USER1 of the VM host 10. Also, on the remote system 20, a second profile and second key is defined for a second user GUEST of the hosted OS 25 of the VM host 10.

[00019] On the VM host, matching profiles and key are also defined. In other words, on the VM host 10, a first profile and first key is defined for a first user USER1 of the VM host 10, wherein the first profile and first key on the VM host 10 match the first profile and first key of the remote system 20. Similarly, on the VM host 10, a second profile and second key

is defined for a second user GUEST of the hosted OS 25, wherein the second profile and second key on the VM host 10 match the second profile and second key of the remote system 20.

[00020] Access to generate keys/passwords can be tightly controlled by a Resource Access Control Facility (RACF) on all three systems (the VM host 10, the remote control system 20, and the hosted OS 25). The RACF may generate single-use passwords for secure network requests.

[00021] An authorised user USER-ID of the remote system 20 uses a dialog to request an IPL (as indicated by the arrow labelled "A"). The requested IPL can be requested to be immediate or can be scheduled for a particular time.

[00022] At the appropriate time, a control program in the IPL server 30 of the remote control system 20 creates a pass key for the second user GUEST of the hosted OS 25 using the second key of the remote system 20. The IPL server 30 then creates a shut-down instruction using the pass key as a password for the second user GUEST, and subsequently sends the shut-down instruction to (the second user GUEST on) the hosted OS 25 (as indicated by the arrow labelled "B"). The transmitted shut-down instruction commands the hosted OS 25 to close. Consequently, upon receipt of the shut-down instruction at hosted OS 25, the authenticity of the pass key is checked and, if authenticated, the shut-down instruction is executed by the hosted OS 25 and the hosted OS 25 shuts-down.

[00023] After the hosted system is shut-down, the remote control system 20 creates a pass key for the first user USER1 of the VM host 10 using the first key of the remote system 20. The IPL server 30 then creates a record using the pass key for the first user USER1 as a password for the first user USER1. The records comprises: an identification of the hosted OS 25; an IPL request; the pass key for the first user USER1; and identification of the requesting party (e.g. USER-ID)

[00024] The generated record is then transmitted from the IPL server 30 to the first user USER1 of the VM host 10 (as indicated by the arrow labelled "C"). Upon receipt of the

record, the authenticity of the pass key of the record is checked and, if authenticated, the requested IPL is executed so as to restart the hosted OS 25 (as indicated by the arrow labelled "D").

[00025] Referring now to Figure 2, there is shown a flow diagram of an embodiment of the invention. The flow diagram is illustrated with two sides (one for the remote system and one for the VM host) so as to indicate where each step is implemented. In other words, the flow diagram indicates which part of a system according to an embodiment undertakes a particular step based on which side of the flow diagram the step is located. It will, however, be appreciated that this is purely exemplary of a particular embodiment and that other embodiments may undertake one or more steps may be undertaken at different locations and/or by different parts/components.

[00026] In step 200, a first profile and first key for a first user of the VM host is defined on the remote system. Similarly, in step 205, the first profile and first key for the first user is also defined on the VM-host. Thus, the same (i.e. matching) first profiles and first keys are defined on both the remote system and the VM-host.

[00027] In step 210, a second profile and second key for a second user of the hosted OS is defined on the remote system. Similarly, in step 215, the second profile and second key for the second user of the hosted OS is also defined on the VM hosted system. Thus, the same (i.e. matching) second profiles and second keys are defined on both the remote system and the VM-hosted system.

[00028] In step 220, it is determined if an IPL is requested by a user of the remote system. If no IPL request is made, the method returns to step 220 whereby it is again determined if an IPL request is made. In other words, the method repeatedly undertakes step 220 to monitor for the occurrence of an IPL request.

[00029] When, at step 220, it is determined that an IPL request has been made by a user of the remote system, the method proceeds to step 225.

[00030] Based on the detected IPL request, the remote system generates a shut-down instruction and transmits the generated shut-down instruction to the VM-hosted system in step 225. Here, the shut-down instruction is generated so as to comprise a first authentication key for the second user of the hosted OS, the first authentication key being created from using the second key of the remote system 20.

[00031] Next, in step 227, the IPL request is received at the VM-hosted system and verified by checking the first authentication key of the IPL request. If the first authentication key of the IPL request is determined to be invalid, the IPL request is ignored by the VM hosted system and the method simply returns to step 220. If, on the other hand, the first authentication key of the IPL request is determined to be valid, the method proceeds to step 230 wherein the shut-down instruction is executed by the VM-hosted system so as to shut down the VM-hosted system.

[00032] In step 235, the remote system confirms that the VM-hosted system has been shut down as expected. This may be done by simply waiting for a predetermined amount of time or may be actively confirmed by pinging the VM-hosted system and checking for a response, for example. Other methods to ensure that the VM-hosted system has been shut down before the method proceeds further may be used.

[00033] Once it has been confirmed in step 235 that the VM-hosted system is shut-down, the method proceeds to step 240 in which a data file is generated and transmitted to the first user of the VM host. Here, the data file is generated so as to comprise an IPL request for the VM-hosted system a second authentication key for first user of the VM host.

[00034] Next, in step 245, the data file is received by the first user of the VM-host and verified by checking its second authentication key. If the second authentication key of the data file is determined to be invalid, the data file is ignored. If, on the other hand, the second authentication key of the data file is determined to be valid, the IPL request of the data file is executed so as to restart the VM-hosted system.

[00035] Referring now to Figure 3, there is shown a schematic block diagram of system 300 according to an embodiment of the invention. The system 300 comprises a control client

device 310 that is adapted to have remote access to a server 320 via a network 330. The server 320 comprises a processor 340 runs a VM which hosts an OS 350 for a user 360 to access via the network 330.

[00036] The control client device 310 comprises an IPL server 370 which is adapted to receive an access request from the user 360. In response to receiving such an access request, the IPL server 370 generates a shut-down instruction and transmits it to the VM-hosted system 350. The shut-down instruction comprises a first set of authentication details generated from authentication information stored in the control client device 310 (or provided to the control client device 310 by the user 360).

[00037] The hosted system 350 receives the shut-down instruction from the control client device 310 (via the network 330) and verifies the first set of authentication details of the shut-down instruction. If the first set of authentication details are verified as being authentic (e.g. trusted, correct or equal to a first set of authentication details stored by the server 320), the processor executes the shut-down instruction to shut-down the VM-hosted OS 350.

[00038] The IPL server 370 also generates an IPL file and transmits the IPL file to the server 320 after the VM-hosted OS 350 has been shut-down. The IPL file comprises: an IPL request, a second set of authentication details; identification details of the VM-hosted OS; and identification details of the user 360.

[00039] The processor 340 of the server 320 receives the IPL file from the control client device 310 (via the internet 330) and verifies the second set of authentication details of the IPL file. If the second set of authentication details are verified as being authentic (e.g. trusted, correct or equal to a second set of authentication details stored by the server 320), the processor executes the IPL request of the IPL file to re-start the VM-hosted OS 350.

[00040] It will be clear to one of ordinary skill in the art that all or part of the method of one embodiment of the present invention may suitably and usefully be embodied in a logic apparatus, or a plurality of logic apparatus, comprising logic elements arranged to perform

the steps of the method and that such logic elements may comprise hardware components, firmware components or a combination thereof.

[00041] It will be equally clear to one of skill in the art that all or part of a logic arrangement according to one embodiment of the present invention may suitably be embodied in a logic apparatus comprising logic elements to perform the steps of the method, and that such logic elements may comprise components such as logic gates in, for example a programmable logic array or application-specific integrated circuit. Such a logic arrangement may further be embodied in enabling elements for temporarily or permanently establishing logic structures in such an array or circuit using, for example, a virtual hardware descriptor language, which may be stored and transmitted using fixed or transmittable carrier media.

[00042] It will be appreciated that the method and arrangement described above may also suitably be carried out fully or partially in software running on one or more processors (not shown in the figures), and that the software may be provided in the form of one or more computer program elements carried on any suitable data-carrier (also not shown in the figures) such as a magnetic or optical disk or the like. Channels for the transmission of data may likewise comprise storage media of all descriptions as well as signal-carrying media, such as wired or wireless signal-carrying media.

[00043] A method is generally conceived to be a self-consistent sequence of steps leading to a desired result. These steps require physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It is convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, parameters, items, elements, objects, symbols, characters, terms, numbers, or the like. It should be noted, however, that all of these terms and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

[00044] The present invention may further suitably be embodied as a computer program product for use with a computer system. Such an implementation may comprise a series of computer-readable instructions either fixed on a tangible medium, such as a computer readable medium, for example, e.g. a CD-ROM, DVD, USB stick, memory card, network-area storage device, internet-accessible data repository, and so on, or transmittable to a computer system, via a modem or other interface device, over either a tangible medium, including but not limited to optical or analogue communications lines, or intangibly using wireless techniques, including but not limited to microwave, infrared or other transmission techniques. The series of computer readable instructions embodies all or part of the functionality previously described herein.

[00045] Those skilled in the art will appreciate that such computer readable instructions can be written in a number of programming languages for use with many computer architectures or operating systems. Further, such instructions may be stored using any memory technology, present or future, including but not limited to, semiconductor, magnetic, or optical, or transmitted using any communications technology, present or future, including but not limited to optical, infrared, or microwave. It is contemplated that such a computer program product may be distributed as a removable medium with accompanying printed or electronic documentation, for example, shrink-wrapped software, pre-loaded with a computer system, for example, on a system ROM or fixed disk, or distributed from a server or electronic bulletin board over a network, for example, the Internet or World Wide Web.

[00046] In one alternative, one embodiment may be realized in the form of a computer implemented method of deploying a service comprising steps of deploying computer program code operable to cause the computer system to perform all the steps of the method when deployed into a computer infrastructure and executed thereon.

[00047] In a further alternative, one embodiment may be realized in the form of a data carrier having functional data thereon, the functional data comprising functional computer data structures to, when loaded into a computer system and operated upon thereby, enable the computer system to perform all the steps of the method.

[00048] The flowchart and block diagram in the above figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

[00049] While one or more embodiments have been illustrated in detail, one of ordinary skill in the art will appreciate that modifications and adaptations to those embodiments may be made.

[00050] Other variations to the disclosed embodiments can be understood and effected by those skilled in the art in practising the claimed invention, from a study of the drawings, the disclosure, and the appended claims. In the claims, the word "comprising" does not exclude other elements or steps, and the indefinite article "a" or "an" does not exclude a plurality. A single processor or other unit may fulfil the functions of several items recited in the claims. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measured cannot be used to advantage. Any reference signs in the claims should not be construed as limiting the scope.

CLAIMS

1. A method for providing authorized remote access to initial program load, IPL, an operating system hosted by a virtual machine, VM, the method comprising:

receiving, at a client system, a request for an IPL of an operating system hosted by a VM, the VM being provided by a server system;

generating, at the client system, a first authentication token and a shut-down instruction for shutting down the operating system;

communicating the first authentication token and the shut-down instruction to the server system;

at the server system, verifying that the first authentication token is valid and, if valid, executing the shut-down instruction on the server system to shut-down the operating system;

generating, at the client system, a second authentication token and an IPL instruction for the operating system;

communicating the second authentication token and the IPL instruction to the server; and

at the server system, verifying that the second authentication token is valid and, if valid, executing the IPL instruction on the server to re-start the operating system.

2. The method of claim 1, further comprising the step of, prior to generating a second authentication token and an IPL instruction for the operating system, monitoring the operating system to determine when the operating system is completely shut-down.

3. The method of claim 1 or 2, wherein the shut-down instruction further comprises at least one of: an identification of a user of the client system; and an identification of the operating system.

4. The method of claim 1, 2 or 3, wherein the IPL instruction further comprises at least one of: an identification of a user of the client system; and an identification of the operating system.

5. The method of any preceding claim, wherein at least one of: the first authentication token; and the second authentication token is generated based on at least one of: the received request for an IPL; and authentication information provided by the client system or a user of the client system.

6. The method of any preceding claim, wherein at least one of: the first authentication token; and the second authentication token comprises a one-time use pass key adapted to be rendered invalid when its validity has been checked.

7. A computer program product for providing authorized remote access to an operating system hosted by a VM, wherein the computer program product comprises a computer-readable storage medium having computer-readable program code embodied therewith, the computer-readable program code configured to perform all of the steps of any of claims 1 to 6.

8. A computer system comprising: a computer program product according to claim 7; and one or more processors adapted to perform all of the steps of any of claims 1 to 6.

9. A client system for providing authorized remote access to an operating system hosted by a VM of a server system, the client system comprising:

IPL request unit adapted to receive a request for an IPL of an operating system hosted by the VM, to generate a first authentication token and a shut-down instruction for shutting down the operating system, and to generate a second authentication token and an IPL instruction for re-starting the operating system; and

a communication interface adapted to communicate the first authentication token and the shut-down instruction to the server system, and to communicate the second authentication token and the IPL instruction to the server.

10. The client system of claim 9, wherein the client system is adapted to monitor the operating system to determine when the operating system is completely shut-down.

and wherein the communication interface is adapted to communicate the second authentication token and the IPL instruction to the server after it has been determined that the operating system is completely shut-down.

11. The client system of claim 9 or 10, wherein at least one of: the shut-down instruction; and the IPL instruction further comprises at least one of: an identification of a user of the client system; and an identification of the operating system.

12. The client system of any of claims 9 to 11, wherein the IPL request module is adapted to generate at least one of: the first authentication token; and the second authentication token is based on at least one of: the received request for an IPL; and authentication information provided by the client system or a user of the client system.

13. A server system for providing authorized remote access to an operating system hosted by a VM of the server system, the client system comprising:

a communication interface adapted to receive, from a client system, a first authentication token and a shut-down instruction for shutting down the operating system, and to receive, from the client system, a second authentication token and an IPL instruction for re-starting the operating system;

a verification unit adapted to verify that the first authentication token is valid and to verify that the second authentication token is valid; and

a processor adapted to execute the shut-down instruction on the server system to shut-down the operating system if the verification unit verifies that the first authentication token is valid, and to execute the IPL instruction to re-start the operating system if the verification unit verifies that the second authentication token is valid.

14. The server system of claim 13, wherein the shut-down instruction further comprises at least one of: an identification of a user of the client system; and an identification of the operating system,

and wherein the verification unit is adapted to verify that the first authentication token is valid based on at least one of an identification of a user of the client system; and an identification of the operating system.

15. The server system of claim 13 or 14, wherein the IPL instruction further comprises at least one of: an identification of a user of the client system; and an identification of the operating system,

and wherein the verification unit is adapted to verify that the second authentication token is valid based on at least one of: an identification of a user of the client system; and an identification of the operating system.