(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 472 719 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
04.08.2021 Bulletin 2021/31

(21) Application number: **17816133.7**

(22) Date of filing: **21.06.2017**

(51) Int Cl.:
H04L 29/06 *(2006.01)* ***G06F 17/00*** *(2019.01)*
G06F 15/16 *(2006.01)* ***H04W 12/065*** *(2021.01)*
H04W 12/06 *(2021.01)*

(86) International application number:
PCT/US2017/038526

(87) International publication number:
WO 2017/223190 (28.12.2017 Gazette 2017/52)

(54) **METHOD AND APPARATUS OF IMPLEMENTING A VPN TUNNEL**

VERFAHREN UND VORRICHTUNG ZUR IMPLEMENTIERUNG EINES VPN-TUNNELS

PROCÉDÉ ET APPAREIL PERMETTANT DE METTRE EN OEUVRE UN TUNNEL DE RÉSEAU VPN

(84) Designated Contracting States:
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

(30) Priority: **21.06.2016 US 201662352759 P**

(43) Date of publication of application:
24.04.2019 Bulletin 2019/17

(73) Proprietor: **Noa, Inc.**
Miami Beach, FL 33140 (US)

(72) Inventors:
- **MCNEELY, Mark**
  Miami
  FL 33125 (US)
- **MCNEELY, Michael**
  Miami
  FL 33125 (US)

(74) Representative: **Barker Brettell LLP**
100 Hagley Road
Edgbaston
Birmingham B16 8QQ (GB)

(56) References cited:
US-A1- 2009 319 782
US-A1- 2013 091 537
US-A1- 2015 312 041
US-A1- 2016 125 180
US-A1- 2009 319 782
US-A1- 2013 091 537
US-A1- 2015 312 041
US-A1- 2016 125 180

EP 3 472 719 B1

Description

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The present invention is directed to allowing a more secure initial, and continuous authentication of virtual private network (VPN) tunneling. The device of the present invention contains its own microprocessor and operating system which connects to the host system via a universal serial bus (USB). The present invention involves executing and storing of the VPN software, certificates, credentials and sensors on the device, which allows for more security and manageability as opposed to executing the VPN on the host system. The device can be configured for Login, Quick Response (QR) Codes, Near-Field Communication (NFC) or Bluetooth Low Energy (LE) proximity authentication to activate or deactivate the VPN tunnel.

2. Description of the Related Art

[0002] A VPN system allows users to send/receive data across shared or public networks, over the internet, as if their computers were directly connected to a private network. The VPN tunnel is a secure, encrypted connection, between the user's client computer and computers and/or servers operated by the VPN service.

[0003] Traditional VPN tunnels (i.e., Internet Protocol Security Standards, such as RFC2547, and RFC4364) require software, certificate and password information to be installed on the personal computer (PC) (i.e., desktop, laptop, etc.) of the user. However, this approach has the risk of the user's computer being hacked since all the information is stored there. Another risk is if the user's computer is stolen with the certificates and passwords on the computer itself, then this would leave the network behind the VPN server vulnerable until the certificates were revoked.

[0004] In other concerns, once the user logs into the personal, client computer, the VPN tunnel can be opened automatically or by the user logging in with the tunnel application. However, once the user walks away from the computer, the tunnel is still open with the computer unlocked, and anyone can walk up to the computer and access the VPN network. Another scenario of concern is where the user locks the computer and someone uses a remote desktop platform (RDP) into the computer to access the tunnel.

[0005] Specifically, in a traditional, installed VPN client computer, the certificates, passwords, and endpoint information are stored in software on the operating system (OS) drive. The OS drive is installed on the user's client computer, and the VPN tunnel accesses the internet via the network information center (NIC). The Internet Protocol Suite (TCP/IP) application accesses the VPN tunnel by IP or hostname, but first accesses the VPN software, and the TCP/IP application accessing the internet by IP or hostname, proceeds via a default gateway to the NIC before reaching the internet. These certificates, passwords, and endpoint information are vulnerable if the desktop or laptop is stolen or hacked.

[0006] Thus, a way of securing the VPN tunnel and the certificates, passwords, and endpoint information in software on the OS drive on the client computer, is desired.

[0007] US 2009/0319782 A1 discloses an interconnectable personal computer architecture comprising secure, portable and persistent computing environments that provide secure computing sessions with persistence. The computing environments are implemented using a secure non-computing client device, such as a USB device, that interfaces with a host computer and, optionally, a trusted server. The secure non-computing client device is used to instantiate a secure BIOS and a secure cold or warm boot of the host computer, from the client device, in a host protected area of the host computer, or from the trusted server.

[0008] US 2013/0091537 A1 discloses restricting network and device access based on presence detection, in which a network policy is applied responsive to specified events, or triggers, to a networked device. If a specified event occurs, the network policy may restrict the device's access to the network.

SUMMARY OF THE INVENTION

[0009] The present invention, which is defined by the appended claims, is directed to allowing a more secure initial, and continuous authentication of virtual private network (VPN) tunneling. The controller of the present invention contains its own microprocessor and operating system which connects to the host system via a universal serial bus (USB) or via another mode of securing coupling. The present invention involves executing and storing of the VPN software, certificates, credentials and sensors on the device, which allows for more security and manageability as opposed to executing the VPN on the host system. The controller device can be configured for primary and continuous authentication of the presence of the user via biometrics or interactivity with the user, or for primary and continuous authentication by a second trusted device, such as a smartphone, smartwatch, near-field communication (NFC) ring, or custom device, which continuous authentication uses Quick Response (QR) Codes, Near-Field Communication (NFC) or Bluetooth Low Energy (LE) proximity authentication. The controller activates the VPN tunnel upon primary authentication and deactivates the VPN tunnel when continuous authentication fails.

[0010] In one embodiment, a virtual private network (VPN) tunnel system includes: a controller which is coupled to a client computer, the controller including a microprocessor containing at least one memory, the memory containing an operating system program; wherein the memory stores authentication information including cer-

tificate, password and endpoint information in the controller instead of in a database of the client computer; and wherein when the authentication information received by the client computer is validated by the controller, the microprocessor executes the operating system program of the controller to implement at least one VPN tunnel which connects the client computer to a VPN server and to a private network of computers and servers, via an internet connection.

[0011] In one embodiment, the primary and continuous authentication of the controller is performed by at least one of periodic input of biometrics of a user, or communications with a secondary device via at least one contactless communication system.

[0012] The controller is disposed in a universal serial bus (USB) VPN device.

[0013] In one embodiment, the contactless communication system includes one of Bluetooth Low Energy (LE), Near-Field Communication (NFC), or Quick Response (QR) Code

[0014] In one embodiment, the VPN tunnel is deactivated immediately when one of inactivity over a predetermined period of time occurs at the client computer, incorrect biometrics are received at the client computer, uncoupling of the controller from the client computer occurs, or lack of proximity of the secondary device from the client computer occurs.

[0015] In one embodiment, the controller automatically deactivates upon intrusion detection and deletes all secured data in the memory.

[0016] In one embodiment, the secondary device includes one of a portable or wearable device, including one of a smartphone, a smartwatch, an NFC ring, or a custom device with a microprocessor.

[0017] In one embodiment, the memory stores encryption private keys.

[0018] In one embodiment, the secondary device is equipped with wireless capability; wherein the secondary device emits a signal to the controller using the wireless capability, in order to activate the VPN tunnel once the controller is coupled to the client computer.

[0019] In one embodiment, an authentication applet is preinstalled on the secondary device; and wherein a password is received in the secondary device upon an authentication request, and the signal is transmitted to the controller, which returns an authentication token to the secondary device; and wherein once the authentication token is received from the controller and is valid, and when the operating system program is configured for remote authentication, the authentication token is forwarded by the secondary device to an authentication server for authorization.

[0020] In one embodiment, the VPN tunnel remains activated for as long as the secondary device is sending the signal to the controller, and the secondary device is within a predetermined range from the client computer; and wherein when the secondary device is out of range of the controller, the VPN tunnel is terminated.

[0021] In one embodiment, the predetermined range is determined using Received Signal Strength Indication (RSSI) with one of Bluetooth LE, or a limited range of NFC.

[0022] In one embodiment, the system further includes: a status indicator disposed on the USB VPN device, which indicates at least one of a connected status or a security status of the USB VPN device.

[0023] In one embodiment, the USB VPN device further includes an optical sensor to read Quick Response (QR) codes for authentication.

[0024] In one embodiment, a method of implementing a virtual private network (VPN) tunnel system, includes: coupling a controller to a client computer; wherein the controller includes a microprocessor containing at least one memory which contains an operating system program; wherein the memory stores certificate, password and endpoint information in the controller instead of in a database of the client computer; and receiving authentication information at the client computer; validating said authentication information using the controller; and executing the operating system program of the controller to implement at least one VPN tunnel which connects the client computer to a VPN server and to a private network of computers and servers, via an internet connection.

[0025] In one embodiment, the method further includes: performing primary and continuous authentication of the controller is performed by at least one of periodic input of biometrics of a user, or communications with a secondary device via at least one contactless communication system.

[0026] In one embodiment, the method further includes: deactivating the VPN tunnel immediately when one of inactivity over a period of time occurs at the client computer, incorrect biometrics are received at the client computer, uncoupling of the controller from the client computer occurs, or lack of proximity of the secondary device from the client computer occurs.

[0027] In one embodiment, the method further includes: deactivating the controller automatically upon intrusion detection and deleting all secured data in the memory.

[0028] In one embodiment, the method further includes: emitting a signal to the controller using wireless capability of the secondary device, in order to activate the VPN tunnel once the controller is coupled to the client computer.

[0029] In one embodiment, the method further includes: preinstalling an authentication applet on the secondary device; and receiving a password in the secondary device upon an authentication request, and transmitting the signal to the controller; returning an authentication token to the secondary device; validating the authentication token; and forwarding the authentication token to an authentication server for authorization when the operating system program is configured for remote authentication.

[0030] Thus, has been outlined, some features con-

sistent with the present invention in order that the detailed description thereof that follows may be better understood, and in order that the present contribution to the art may be better appreciated. There are, of course, additional features consistent with the present invention that will be described below and which will form the subject matter of the claims appended hereto.

[0031] In this respect, before explaining at least one embodiment consistent with the present invention in detail, it is to be understood that the invention is not limited in its application to the details of construction and to the arrangements of the components set forth in the following description or illustrated in the drawings. Methods and apparatuses consistent with the present invention are capable of other embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein, as well as the abstract included below, are for the purpose of description and should not be regarded as limiting.

[0032] As such, those skilled in the art will appreciate that the conception upon which this disclosure is based may readily be utilized as a basis for the designing of other structures, methods and systems for carrying out the several purposes of the present invention. It is important, therefore, that the claims be regarded as including such constructions insofar as they do not depart from the scope of the methods and apparatuses as defined by the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033]

FIG. 1 is a schematic diagram of a VPN tunnel system according to one embodiment consistent with the present invention.

FIG. 2 is a schematic diagram of the installed VPN client of the VPN tunnel system of FIG. 1, showing where the certificates, passwords, and endpoint information are held, according to one embodiment consistent with the present invention.

FIG. 3 is a schematic diagram showing the USB VPN device of the present invention installed in a computer USB port, and a smart phone which can be used with the USB VPN device, according to one embodiment consistent with the present invention.

FIG. 4 is a schematic diagram showing the authentication process of the USB VPN device, according to one embodiment consistent with the present invention.

FIG. 5 is a schematic diagram showing the authentication process of FIG. 4, according to one embodiment consistent with the present invention.

DESCRIPTION OF THE INVENTION

[0034] The present invention is directed to allowing a more secure initial, and continuous authentication of virtual private network (VPN) tunneling. The controller of the present invention contains its own microprocessor and operating system which connects to the host system via a universal serial bus (USB) or via another mode of securing coupling. The present invention involves executing and storing of the VPN software, certificates, credentials and sensors on the device, which allows for more security and manageability as opposed to executing the VPN on the host system. The controller device can be configured for primary and continuous authentication of the presence of the user via biometrics or interactivity with the user, or for primary and continuous authentication by a second trusted device, such as a smartphone, smartwatch, nearfield communication (NFC) ring, or custom device, which continuous authentication uses Quick Response (QR) Codes, Near-Field Communication (NFC) or Bluetooth Low Energy (LE) proximity authentication. The controller activates the VPN tunnel upon primary authentication and deactivates the VPN tunnel when continuous authentication fails.

[0035] In one embodiment, the VPN tunnel system 100 of the present invention (see FIG. 1) includes VPN tunnels 105 (i.e., Internet Protocol Security Standards, such as RFC2547, and RFC4364) which connect a user's client computer (i.e., laptop 102 or desktop 103) via the internet 104 to a VPN server 106, and a private network (i.e., computer(s) 107, and server(s) 108).

[0036] In order to prevent security issues with the certificate, password and endpoint information, being normally held in the databases of the memory installed on the operating system (OS) of the personal computer (PC) 102, 102, the present invention provides a universal serial bus (USB) VPN device 101, which includes the operating system (OS) software program which runs on the device 101, rather than on the user's computer 102, 103.

[0037] Since the certificates, passwords and endpoint information are installed on the USB device 101 rather than on the computer 102, 103, and all that is needed on the computer 102, 103 is an internet protocol (IP) and a route 202 (see FIG. 2) from Internet Protocol Suite (TCP/IP) application 203 (accessing the VPN tunnel 204 by IP or hostname) to the VPN USB device 201, which can be set using driver setup or net, ipconfig and route commands. All the VPN tunnel data passes into the USB VPN device 101 via the USB connector/port 110 then is routed back out the USB VPN tunnel device 101 through the same USB connector/port 110.

[0038] As shown in FIG. 2, the TCI/IP application 205 accessing the internet does so via the default gateway 206 to the network information center (NIC) 207. Accordingly, the certificates, passwords, and endpoint information are no longer vulnerable if the client computer 102, 103 is stolen or hacked.

[0039] Once the USB VPN device 101 is plugged into

the USB port 110 of the client computer 102, 103, and powered up, the USB VPN device tunnel 105, 204 would be in the non-connected state. In one embodiment, primary and continuous authentication of the USB VPN device 101 can be performed by one or more of web Login, biometrics, wireless (i.e., Bluetooth LE, NFC), or Quick Response (QR) Code (described further below). All Login, NFC, Bluetooth LE, Biometrics, or QR Codes are encrypted using well established standards.

[0040] In one embodiment, once authentication is achieved, the VPN tunnel 105, 204 would start the protocol negotiation and changes to the connected state, if the software program determines that the device certificates and endpoint certificates match.

[0041] In one embodiment, the VPN tunnel 105, 204 is easy to open/close by simply inserting the USB VPN device 101 into the port 110 of the client computer 102, 103, and when the USB VPN device 101 is not desired to be in use, the USB VPN device 101can be removed from the port 110 of the client computer 102, 103, and since the VPN tunnel 105, 204 runs on the operating system installed on the USB VPN device 101, the VPN tunnel 105, 204 is instantly shutdown.

[0042] In one embodiment, the operating system software program which runs the VPN tunnel 105, 204, is installed, secured, and run on its own microprocessor within the USB VPN device 101. Thus, as stated above, other than driver and routing information, no other software needs to be installed on the client computer 102, 103, providing security of the certificates, password, and endpoint information.

[0043] In one embodiment, the controller of the USB VPN device 101 can be configured to different levels of security. Further, in one embodiment, upon intrusion detection (i.e. hacking, etc.), the controller of the USB VPN device 101 can be configured to automatically deactivate and to delete all secured data in microprocessor memory.

[0044] In one embodiment, status indicators 310 (see FIG. 4) are included such that the user or other personnel can determine the status of the USB VPN device 101 (i.e., on, off, security issue, etc.).

[0045] In one embodiment, encryption private keys are stored on the USB VPN device 101, and the USB VPN device 101 can connect to commonly used firewalls 109 or VPN servers 108.

[0046] In one embodiment, the user or information technology personnel can perform easy administration using onboard webserver protocol, which can be permanently deactivated once configuration is completed. As noted above, configuration parameters include NFC data, biometric data, authentication endpoints, VPN endpoints, certificates, etc. Thus, the USB VPN device 101 of the present invention is simple for users to understand and utilize.

[0047] In one embodiment, the method of implementing a VPN tunnel system, begins with the administrator/user plugging in the USB VPN device 300 (see FIG. 3) into the USB port 304 of the administrator's client computer 301.

In step 1), the administrator uploads the operating system (OS) stored on the USB VPN device 300 into the client computer 301.

In step 2), the administrator navigates to the administration URL on the client computer 301 screen.

In step 3), the administrator authenticates by biometrics, etc., into the onboard webserver of said client computer 301.

In step 4), if the authentication of said biometrics or other authentication information inputted into said client computer 301, is confirmed by said controller of said USB VPN device 300, the administrator enters the USB VPN device 300 information into the client computer 301.

In step 5), the administrator deactivates the onboard administration webserver. Once the onboard administration webserver is deactivated, the administrator uploads a new USB VPN device 300 operating system (OS) image and reconfigures the USB VPN device 300.

In step 6), the administrator implements the frequency and protocols of the continuous and periodic authentication required to compel proper authentication of the user or a category of users.

[0048] In this way, when the VPN tunnel 309 is activated in step 7), after proper authentication as above, the user must enter biometric or other authentication information, such as from a second trusted device (i.e., smartphone, smartwatch, nearfield communication (NFC) ring, or custom device), into the client computer 301, on a continuous and periodic basis, in order to keep the VPN tunnel 309 open. If this information is not provided or is faulty, or the controller notes inactivity of the user over a predetermined period of time, or lack of proximity of authentication (i.e., using Quick Response (QR) Codes, Near-Field Communication (NFC) or Bluetooth Low Energy (LE)), the controller will immediately deactivate the VPN tunnel 309.

[0049] In an optional step 7), the administrator can activate an onboard security system which deactivates the USB VPN device 300 if unauthorized access is detected (hacking), and the secure data thereon is deleted. Once tripped, the USB VPN device 300 would need to be re-imaged and configured.

[0050] In another embodiment consistent with the present invention, a contactless communication system is used to activate the VPN tunnel. In this exemplary embodiment, a Bluetooth LE or an NFC capable smartphone (cell phone) 302 sends a signal 303 to the USB VPN device 300, in order to activate the VPN tunnel, once the

USB VPN device 300 is plugged into the USB port 304 of the client computer 301 (see FIGS. 3-5).

In step a), the signal 303 boots/powers up the VPN operating system (OS).

In step b), when fully powered up, the connection indicator 310 on the USB VPN device 300, if present, will display red to indicate it is ready for authentication.

In step c), at this point, the user can start the authentication applet which is preinstalled on the smartphone 302.

In step d) the smartphone 302 will present an authentication request, and after the user enters the required password into the application, the smartphone 302 will transmit an encrypted signal to the USB VPN device 300, which will return an authentication token to the smart phone 302.

In step e), once a valid authentication token is received from the USB VPN device 300, and if the system is configured for remote authentication, the token will be forwarded by the smartphone 302 to the authentication server 305 for authorization.

In step f), once authorized by the authentication server 305, the smart phone application will transmit an encrypted signal to the USB VPN device 300, with authorization to connect the VPN tunnel 309. At this point the connection indicator 310 on the USB VPN device 300, if present, will display green. If the system is not configured for remote authentication, the application on the smartphone 302 will validate the token.

In step g), once the authentication information is validated as in steps 3) and 4) above, the VPN tunnel 309 - via VPN server 306 - can be activated from client computer 301 to remote computers, i.e., servers 307, 308. The VPN tunnel 309 will stay activated as long as the smartphone 302 is sending the signal to the USB VPN device 300, and is within a predetermined range (to prevent deterioration of signal strength) from the client computer 301. This continuous, proximity authentication, is another feature of the present invention.

[0051] The predetermined range for the proximity of the smart phone 302 can be determined using Received Signal Strength Indication (RSSI) with Bluetooth LE, or the limited range of NFC. Once the smartphone 302 is out of range of the USB VPN device 300, the RSSI Bluetooth LE or limited range of NFC, the VPN tunnel 309 will be terminated.

[0052] In one embodiment, all data transmitted from the smartphone 302 to the USB VPN device 300 will be encrypted using asymmetric cryptography with the private key stored on the USB VPN device 300. Public key will be stored on the smartphone 302. Data transmitted from the USB VPN device 300 to the smartphone 302 will be symmetric-key block cipher with random keys received from the last transmission from the smartphone 302. The private keys and activation tokens will be generated during the administration process using the onboard web service and stored securely in the memory in the microprocessor of the USB VPN device 300. In order to upload the operating system from the USB VPN device 302 into the client computer 301, and implement imaging and configuration thereof, the web service is deactivated.

[0053] In one embodiment, and as noted above, the USB VPN device 300 will use onboard intrusion detection to protect the VPN tunnel system of the present invention, from unauthorized access. Once an unauthorized attempt is detected by the operating system software program of the VPN tunnel system of the present invention, the VPN tunnel system will delete all secured data in microprocessor memory storage on the USB VPN device 300, and deactivate the USB VPN device 300.

[0054] In one embodiment, as noted above, the USB VPN device 300 runs its software program on its own microprocessor and operating system, which removes the requirement of installing the VPN software, certificates and passwords on the client machine 301.

[0055] In another embodiment consistent with the present invention, the USB VPN device 300 can be equipped with an optical sensor to read Quick Response (QR) codes for authentication in wireless blackout scenarios.

[0056] In this embodiment, the steps i)-iii), are the same as steps a)-c) above.

[0057] In step iv), the smartphone 302 will present an authentication request, and after the user enters the required password into the application, the smartphone 302 will retrieve or generate a QR Code from the authentication server 305, or use one retrieved from the smartphone 302 cache. Once a valid authentication QR code is received by the smartphone 302, and if the VPN tunnel system of the present invention is configured for remote authentication, the token will be forwarded to the authentication server 305 for authorization.

[0058] Steps v) and vi) are the same as steps f) and g) above.

[0059] It should be emphasized that the above-described embodiments of the invention are merely possible examples of implementations set forth for a clear understanding of the principles of the invention. Variations and modifications may be made to the above-described embodiments of the invention without departing from the principles of the invention. All such modifications and variations are intended to be included herein within the scope of the invention and protected by the following claims.

Claims

1. A virtual private network,VPN, tunnel system (100) comprising:

   a client computer (102, 103);
   a universal serial bus, USB, VPN device (101, 201) comprising a controller, said controller coupled to the client computer (102, 103), said controller including a microprocessor containing at least one memory, said memory containing an operating system program;
   wherein said memory stores certificate, password and endpoint information only in said controller instead of in a database of said client computer (102, 103);
   wherein when authentication information received by said client computer (102, 103) is validated by said controller, said microprocessor executes said operating system program of said controller to implement at least one VPN tunnel (105) which connects said client computer (102, 103) to a VPN server (106) and to a private network of computers and servers (107, 108), via an internet connection, and
   wherein said operating system program to implement said at least one VPN tunnel (105) is stored and executed only from said microprocessor of said USB VPN device (101, 201), and
   wherein only driver and routing information is installed on said client computer (102/103).

2. A method of implementing a virtual private network, VPN, tunnel system (100), comprising:

   coupling a controller disposed in a universal serial bus, USB, VPN device (101, 201) to a client computer (102, 103);
   wherein said controller includes a microprocessor containing at least one memory which contains an operating system program; and
   wherein said memory stores certificate, password and endpoint information only in said controller instead of in a database of said client computer (102, 103);
   receiving authentication information at said client computer (102, 103);
   validating said authentication information using said controller; and
   executing said operating system program of said controller to implement at least one VPN tunnel (105) which connects said client computer (102, 103) to a VPN server (106) and to a private network of computers and servers (107, 108), via an internet connection,
   wherein said operating system program to implement said at least one VPN tunnel (105) is stored and executed only from said microprocessor of said USB VPN device (101, 201), and
   wherein only driver and routing information is installed on said client computer (102/103).

3. The system (100) of claim 1 or method of claim 2, wherein primary and continuous authentication of said controller is performed by periodic input of biometrics of a user.

4. The system (100) of claim 1 or method of claim 2, wherein primary and continuous authentication of said controller is performed by communications with a secondary device (302) via at least one contactless communication system.

5. The system (100) or method of claim 4, wherein said contactless communication system includes one of Bluetooth Low Energy, LE, Near-Field Communication, NFC, or Quick Response, QR, Code.

6. The system (100) or method of claim 3, wherein said VPN tunnel (105) is deactivated immediately when one of inactivity over a predetermined period of time occurs at said client computer (102, 103), incorrect biometrics are received at said client computer (102, 103), or uncoupling of said controller from said client computer (102, 103) occurs.

7. The system (100) or method of claim 4, wherein said VPN tunnel (105) is deactivated immediately when one of inactivity over a predetermined period of time occurs at said client computer (102, 103), uncoupling of said controller from said client computer (102, 103) occurs, or lack of proximity of said secondary device from said client computer (102, 103) occurs.

8. The system (100) or method of claim 3 or claim 4, wherein said controller automatically deactivates upon intrusion detection and deletes all secured data in said memory.

9. The system (100) or method of claim 5, wherein said secondary device includes one of a portable or wearable device, including one of a smartphone (302), a smartwatch, an NFC ring, or a custom device with a microprocessor.

10. The system (100) of claim 1 or method of claim 2, wherein said memory stores encryption private keys.

11. The system (100) or method of claim 9, wherein said secondary device (302) is equipped with wireless capability;
    wherein said secondary device (302) emits a signal (303) to said controller using said wireless capability, in order to activate said VPN tunnel (105) once said controller is coupled to said client computer (301).

12. The system (100) or method of claim 11, wherein an authentication applet is preinstalled on said secondary device (302); and
wherein a password is received in said secondary device (302) upon an authentication request, and said signal (303) is transmitted to said controller, which returns an authentication token to said secondary device (302); and
wherein once said authentication token is received from said controller and is valid, and when said operating system program is configured for remote authentication, said authentication token is forwarded by said secondary device (302) to an authentication server (305) for authorization.

13. The system (100) or method of claim 11, wherein said VPN tunnel (105) remains activated for as long as said secondary device (302) is sending said signal to said controller, and said secondary device (302) is within a predetermined range from said client computer (301); and
wherein when said secondary device (302) is out of range of said controller, said VPN tunnel (105) is terminated,
wherein said predetermined range is optionally determined using Received Signal Strength Indication, RSSI, with one of Bluetooth LE, or a limited range of NFC.

14. The system (100) of claim 1 or method of claim 2, further comprising:
a status indicator (304) disposed on said USB VPN device (300), which indicates at least one of a connected status or a security status of said USB VPN device (300).

15. The system (100) or method of claim 9, wherein said USB VPN device (300) further comprises an optical sensor to read Quick Response, QR, codes for authentication.

16. The system (100) of claim 1 or method of claim 2, wherein said controller automatically deactivates an onboard webserver protocol upon completion of configuration of said USB VPN device (300).

17. The system (100) or method of claim 8, wherein said deactivation of said VPN tunnel (105) after said inactivity does not result in destruction of said USB VPN device (300).

Patentansprüche

1. Virtuelles privates Netzwerk, VPN, Tunnelsystem (100), umfassend:

einen Client-Computer (102, 103);

eine universeller serieller Bus, USB, VPN-Vorrichtung (101, 201), die eine Steuereinheit umfasst, wobei die Steuereinheit mit dem Client-Computer (102, 103) gekoppelt ist, wobei die Steuereinheit einen Mikroprozessor beinhaltet, der mindestens einen Speicher enthält, wobei der Speicher ein Betriebssystemprogramm enthält;
wobei der Speicher Zertifikats-, Passwort- und Endpunktinformationen nur in der Steuereinheit anstatt in einer Datenbank des Client-Computers (102, 103) speichert;
wobei, wenn Authentifizierungsinformationen, die von dem Client-Computer (102, 103) empfangen werden, von der Steuereinheit validiert werden, der Mikroprozessor das Betriebssystemprogramm der Steuereinheit ausführt, um mindestens einen VPN-Tunnel (105) zu implementieren, der den Client-Computer (102, 103) mit einem VPN-Server (106) und mit einem privaten Netzwerk von Computern und Servern (107, 108) über eine Internetverbindung verbindet, und
wobei das Betriebssystemprogramm, um den mindestens einen VPN-Tunnel (105) zu implementieren, gespeichert ist und nur von dem Mikroprozessor der USB-VPN-Vorrichtung (101, 201) ausgeführt wird, und
wobei nur Treiber- und Weiterleitungsinformationen auf dem Client-Computer (102/103) installiert sind.

2. Verfahren zum Implementieren eines virtuellen privaten Netzwerk, VPN, Tunnelsystems (100), umfassend:

Koppeln einer Steuereinheit, die in einer universellen seriellen Bus, USB, VPN-Vorrichtung (101, 201) angeordnet ist, mit einem Client-Computer (102, 103);
wobei die Steuereinheit einen Mikroprozessor beinhaltet, der mindestens einen Speicher enthält, der ein Betriebssystemprogramm enthält; und
wobei der Speicher Zertifikats-, Passwort- und Endpunktinformationen nur in der Steuereinheit anstatt in einer Datenbank des Client-Computers (102, 103) speichert;
Empfangen von Authentifizierungsinformationen bei dem Client-Computer (102, 103);
Validieren der Authentifizierungsinformationen unter Verwendung der Steuereinheit; und
Ausführen des Betriebssystemprogramms der Steuereinheit, um mindestens einen VPN-Tunnel (105) zu implementieren, der den Client-Computer (102, 103) mit einem VPN-Server (106) und mit einem privaten Netzwerk von Computern und Servern (107, 108) über eine

Internetverbindung verbindet,
wobei das Betriebssystemprogramm, um den mindestens einen VPN-Tunnel (105) zu implementieren, gespeichert ist und nur von dem Mikroprozessor der USB-VPN-Vorrichtung (101, 201) ausgeführt wird, und
wobei nur Treiber- und Weiterleitungsinformationen auf dem Client-Computer (102/103) installiert sind.

3. System (100) nach Anspruch 1 oder Verfahren nach Anspruch 2, wobei primäre und kontinuierliche Authentifizierung der Steuereinheit durch periodischen Eingabe von Biometrik eines Benutzers durchgeführt wird.

4. System (100) nach Anspruch 1 oder Verfahren nach Anspruch 2, wobei primäre und kontinuierliche Authentifizierung der Steuereinheit durch Kommunikation mit einer sekundären Vorrichtung (302) über mindestens ein kontaktloses Kommunikationssystem durchgeführt wird.

5. System (100) oder Verfahren nach Anspruch 4, wobei das kontaktlose Kommunikationssystem einen beinhaltet von Bluetooth Low Energy, LE, Nahfeldkommunikation, NFC (Near Field Communication) oder Schnellantwort, QR (Quick Response), Code.

6. System (100) oder Verfahren nach Anspruch 3, wobei der VPN-Tunnel (105) unmittelbar deaktiviert wird, wenn eines von Inaktivität über eine vorgegebene Zeitdauer bei dem Client-Computer (102, 103), Empfang inkorrekter Biometrik bei dem Client-Computer (102, 103) oder Entkopplung der Steuereinheit von dem Client-Computer (102, 103) auftritt.

7. System (100) oder Verfahren nach Anspruch 4, wobei der VPN-Tunnel (105) unmittelbar deaktiviert wird, wenn eines von Inaktivität über eine vorgegebene Zeitdauer bei dem Client-Computer (102, 103) auftritt, Entkopplung der Steuereinheit von dem Client-Computer (102, 103) auftritt, oder Mangel an Nähe der sekundären Vorrichtung von dem Client-Computer (102, 103) auftritt.

8. System (100) oder Verfahren nach Anspruch 3 oder Anspruch 4, wobei die Steuereinheit sich bei Eindringungsdetektion automatisch deaktiviert und alle gesicherten Daten in dem Speicher löscht.

9. System (100) oder Verfahren nach Anspruch 5, wobei die sekundäre Vorrichtung eines von einer tragbaren oder am Körper tragbaren Vorrichtung, beinhaltend eines von einem Smartphone (302), einer Smartwatch, einem NFC-Ring oder einer kundenspezifischen Vorrichtung mit einem Mikroprozessor, beinhaltet.

10. System (100) nach Anspruch 1 oder Verfahren nach Anspruch 2, wobei der Speicher private Verschlüsselungsschlüssel speichert.

11. System (100) oder Verfahren nach Anspruch 9, wobei die sekundäre Vorrichtung (302) mit Funkkapazität ausgestattet ist;
wobei die sekundäre Vorrichtung (302) ein Signal (303) an die Steuereinheit unter Verwendung der Funkkapazität aussendet, um den VPN-Tunnel (105) zu aktivieren, sobald die Steuereinheit mit dem Client-Computer (301) gekoppelt ist.

12. System (100) oder Verfahren nach Anspruch 11, wobei eine Authentifizierungsanwendung auf der sekundären Vorrichtung (302) vorinstalliert ist; und
wobei ein Passwort in der sekundären Vorrichtung (302) bei einer Authentifizierungsanfrage empfangen wird und das Signal (303) an die Steuereinheit übertragen wird, die einen Authentifizierungstoken an die sekundäre Vorrichtung (302) zurückschickt; und
wobei, sobald der Authentifizierungstoken von der Steuereinheit empfangen ist und gültig ist, und wenn das Betriebssystemprogramm für Fernauthentifizierung konfiguriert ist, der Authentifizierungstoken von der sekundären Vorrichtung (302) an einen Authentifizierungsserver (305) zur Autorisierung weitergeleitet wird.

13. System (100) oder Verfahren nach Anspruch 11, wobei der VPN-Tunnel (105) so lange aktiviert bleibt, wie die sekundäre Vorrichtung (302) das Signal an die Steuereinheit sendet und die sekundäre Vorrichtung (302) innerhalb einer vorgegebenen Reichweite des Client-Computers (301) ist; und
wobei, wenn die sekundäre Vorrichtung (302) außerhalb der Reichweite der Steuereinheit ist, der VPN-Tunnel (105) beendet wird,
wobei die vorgegebene Reichweite optional unter Verwendung von empfangener Signalstärkenanzeige, RSSI, mit einem von Bluetooth LE oder einer NFC mit begrenzter Reichweite bestimmt wird.

14. System (100) nach Anspruch 1 oder Verfahren nach Anspruch 2, weiter umfassend:
einen Statusindikator (304), der an der USB-VPN-Vorrichtung (300) angeordnet ist, der mindestens einen von einem verbundenen Status oder einem Sicherheitsstatus der USB-VPN-Vorrichtung (300) anzeigt.

15. System (100) oder Verfahren nach Anspruch 9, wobei die USB-VPN-Vorrichtung (300) weiter einen optischen Sensor umfasst, um Schnellantwort, QR, Codes zur Authentifizierung zu lesen.

16. System (100) nach Anspruch 1 oder Verfahren nach

Anspruch 2, wobei die Steuereinheit automatisch ein eingebautes Webserverprotokoll bei Abschluss von Konfiguration der USB-VPN-Vorrichtung (300) deaktiviert.

17. System (100) oder Verfahren nach Anspruch 8, wobei die Deaktivierung des VPN-Tunnels (105) nach der Inaktivität nicht in Zerstörung der USB-VPN-Vorrichtung (300) resultiert.

Revendications

1. Système de tunnel pour réseau privé virtuel, VPN (100) comprenant :

un ordinateur client (102, 103) ;
un dispositif VPN à bus série universel, USB (101, 201) comprenant un dispositif de commande, ledit dispositif de commande étant couplé à l'ordinateur client (102, 103), ledit dispositif de commande incluant un microprocesseur contenant au moins une mémoire, ladite mémoire contenant un programme de système d'exploitation ;
dans lequel ladite mémoire stocke des informations de certificat, de mot de passe et de point final uniquement dans ledit dispositif de commande au lieu d'une base de données dudit ordinateur client (102, 103) ;
dans lequel lorsque des informations d'authentification reçues par ledit ordinateur client (102, 103) sont validées par ledit dispositif de commande, ledit microprocesseur exécute ledit programme de système d'exploitation dudit dispositif de commande pour implémenter au moins un tunnel VPN (105) qui connecte ledit ordinateur client (102, 103) à un serveur VPN (106) et à un réseau privé d'ordinateurs et de serveurs (107, 108), via une connexion Internet, et
dans lequel ledit programme de système d'exploitation pour implémenter ledit au moins un tunnel VPN (105) est stocké et exécuté uniquement à partir dudit microprocesseur dudit dispositif VPN USB (101, 201), et
dans lequel seules des informations de pilote et de routage sont installées sur ledit ordinateur client (102/103).

2. Procédé pour implémenter système de tunnel pour réseau privé virtuel, VPN (100), comprenant les étapes consistant à :

coupler un dispositif de commande disposé dans un dispositif VPN à bus série universel, USB (101, 201) à un ordinateur client (102, 103) ;
dans lequel ledit dispositif de commande inclut un microprocesseur contenant au moins une mémoire qui contient un programme de système d'exploitation ; et
dans lequel ladite mémoire stocke des informations de certificat, de mot de passe et de point final uniquement dans ledit dispositif de commande au lieu d'une base de données dudit ordinateur client (102, 103) ;
recevoir des informations d'authentification au niveau dudit ordinateur client (102, 103);
valider lesdites informations d'authentification en utilisant ledit dispositif de commande ; et
exécuter ledit programme de système d'exploitation dudit dispositif de commande pour implémenter au moins un tunnel VPN (105) qui connecte ledit ordinateur client (102, 103) à un serveur VPN (106) et à un réseau privé d'ordinateurs et de serveurs (107, 108), via une connexion Internet,
dans lequel ledit programme de système d'exploitation pour implémenter ledit au moins un tunnel VPN (105) est stocké et exécuté uniquement à partir dudit microprocesseur dudit dispositif VPN USB (101, 201), et
dans lequel seules des informations de pilote et de routage sont installées sur ledit ordinateur client (102/103).

3. Système (100) selon la revendication 1 ou procédé selon la revendication 2, dans lequel une authentification primaire et continue dudit dispositif de commande est effectuée par une entrée périodique de données biométriques d'un utilisateur.

4. Système (100) selon la revendication 1 ou procédé selon la revendication 2, dans lequel une authentification primaire et continue dudit dispositif de commande est effectuée par des communications avec un dispositif secondaire (302) via au moins un système de communication sans contact.

5. Système (100) ou procédé selon la revendication 4, dans lequel ledit système de communication sans contact inclut l'un parmi Bluetooth Faible Énergie, LE, Communication en Champ-Proche, NFC, ou Code à Réponse Rapide, QR.

6. Système (100) ou procédé selon la revendication 3, dans lequel ledit tunnel VPN (105) est immédiatement désactivé lors d'un événement parmi une inactivité sur une période de temps prédéterminée se produit au niveau dudit ordinateur client (102, 103), des données biométriques incorrectes sont reçues au niveau dudit ordinateur client (102, 103), ou un découplage entre ledit dispositif de commande et ledit ordinateur client (102, 103) se produit.

7. Système (100) ou procédé selon la revendication 4,

dans lequel ledit tunnel VPN (105) est désactivé immédiatement lors d'un événement parmi une inactivité sur une période de temps prédéterminée se produit au niveau dudit ordinateur client (102, 103), un découplage entre ledit dispositif de commande et ledit ordinateur client (102, 103) se produit, ou un manque de proximité dudit dispositif secondaire par rapport audit ordinateur client (102, 103) se produit.

8. Système (100) ou procédé selon la revendication 3 ou la revendication 4, dans lequel ledit dispositif de commande se désactive automatiquement lors d'une détection d'intrusion et supprime toutes les données sécurisées dans ladite mémoire.

9. Système (100) ou procédé selon la revendication 5, dans lequel ledit dispositif secondaire inclut l'un parmi un dispositif portatif ou portable, incluant l'un parmi un smartphone (302), une montre intelligente, une bague NFC, ou un dispositif personnalisé ayant un microprocesseur.

10. Système (100) selon la revendication 1 ou procédé selon la revendication 2, dans lequel ladite mémoire stocke des clés privées de cryptage.

11. Système (100) ou procédé selon la revendication 9, dans lequel ledit dispositif secondaire (302) est équipé d'une capacité sans fil ;
dans lequel ledit dispositif secondaire (302) émet un signal (303) vers ledit dispositif de commande en utilisant ladite capacité sans fil, afin d'activer ledit tunnel VPN (105) une fois que ledit dispositif de commande est couplé audit ordinateur client (301).

12. Système (100) ou procédé selon la revendication 11, dans lequel une applet d'authentification est préinstallée sur ledit dispositif secondaire (302) ; et
dans lequel un mot de passe est reçu dans ledit dispositif secondaire (302) lors d'une demande d'authentification, et ledit signal (303) est transmis audit dispositif de commande, qui renvoie un jeton d'authentification audit dispositif secondaire (302) ; et
dans lequel une fois que ledit jeton d'authentification est reçu en provenance dudit dispositif de commande et est valide, et lorsque ledit programme de système d'exploitation est configuré pour une authentification à distance, ledit jeton d'authentification est renvoyé par ledit dispositif secondaire (302) à un serveur d'authentification (305) pour autorisation.

13. Système (100) ou procédé selon la revendication 11, dans lequel ledit tunnel VPN (105) reste activé aussi longtemps que ledit dispositif secondaire (302) envoie ledit signal audit dispositif de commande, et que ledit dispositif secondaire (302) se trouve dans une portée prédéterminée par rapport audit ordinateur client (301) ; et
dans lequel, lorsque ledit dispositif secondaire (302) est hors de portée dudit dispositif de commande, ledit tunnel VPN (105) est terminé,
dans lequel ladite portée prédéterminée est facultativement déterminée en utilisant une Indication d'Intensité de Signal Reçu, RSSI, avec l'un parmi Bluetooth LE, ou une portée limitée de NFC.

14. Système (100) selon la revendication 1 ou procédé selon la revendication 2, comprenant en outre :
un indicateur d'état (304) disposé sur ledit dispositif VPN USB (300), qui indique au moins l'un parmi un état connecté ou un état de sécurité dudit dispositif VPN USB (300).

15. Système (100) ou procédé selon la revendication 9, dans lequel ledit dispositif VPN USB (300) comprend en outre un capteur optique pour lire des codes à Réponse Rapide, QR, pour authentification.

16. Système (100) selon la revendication 1 ou procédé selon la revendication 2, dans lequel ledit dispositif de commande désactive automatiquement un protocole de serveur Web embarqué lors de l'achèvement d'une configuration dudit dispositif VPN USB (300).

17. Système (100) ou procédé selon la revendication 8, dans lequel ladite désactivation dudit tunnel VPN (105) après ladite inactivité n'entraîne pas une destruction dudit dispositif VPN USB (300).

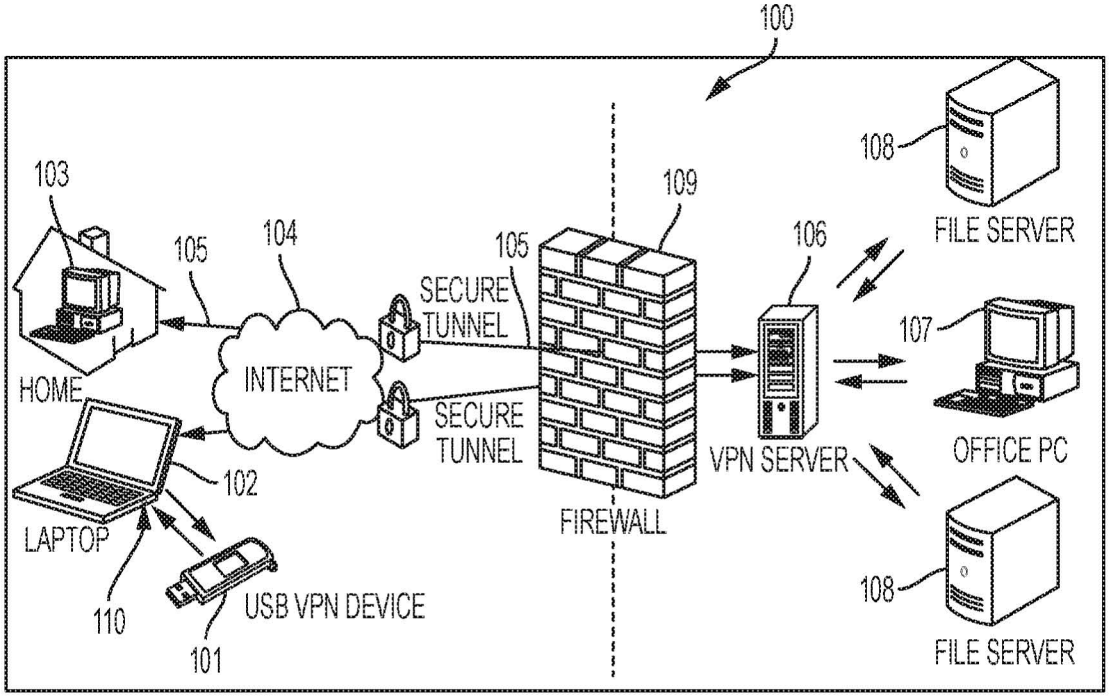
100
103
105
104
105
109
106
108
FILE SERVER
SECURE TUNNEL
107
HOME
INTERNET
SECURE TUNNEL
VPN SERVER
OFFICE PC
102
FIREWALL
LAPTOP
108
USB VPN DEVICE
110
101
FILE SERVER

FIG. 1

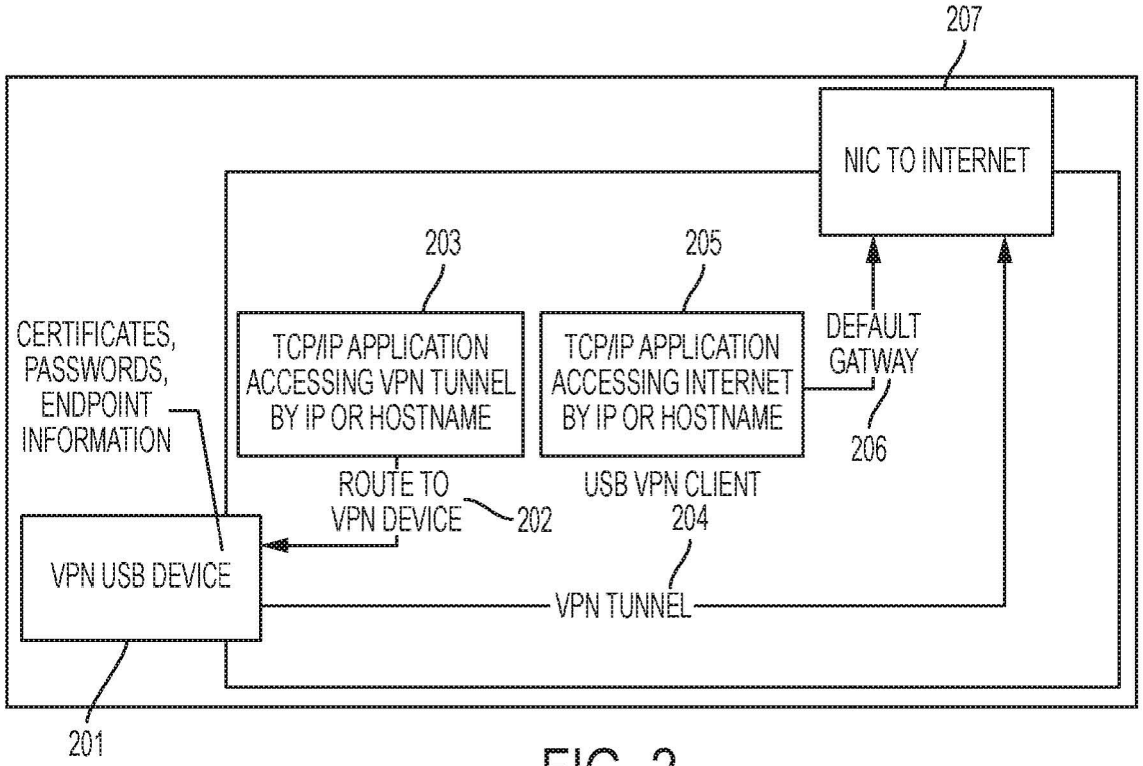
207
NIC TO INTERNET
203
205
CERTIFICATES, PASSWORDS, ENDPOINT INFORMATION
TCP/IP APPLICATION ACCESSING VPN TUNNEL BY IP OR HOSTNAME
TCP/IP APPLICATION ACCESSING INTERNET BY IP OR HOSTNAME
DEFAULT GATWAY
206
ROUTE TO VPN DEVICE
202
USB VPN CLIENT
204
VPN USB DEVICE
VPN TUNNEL
201

FIG. 2

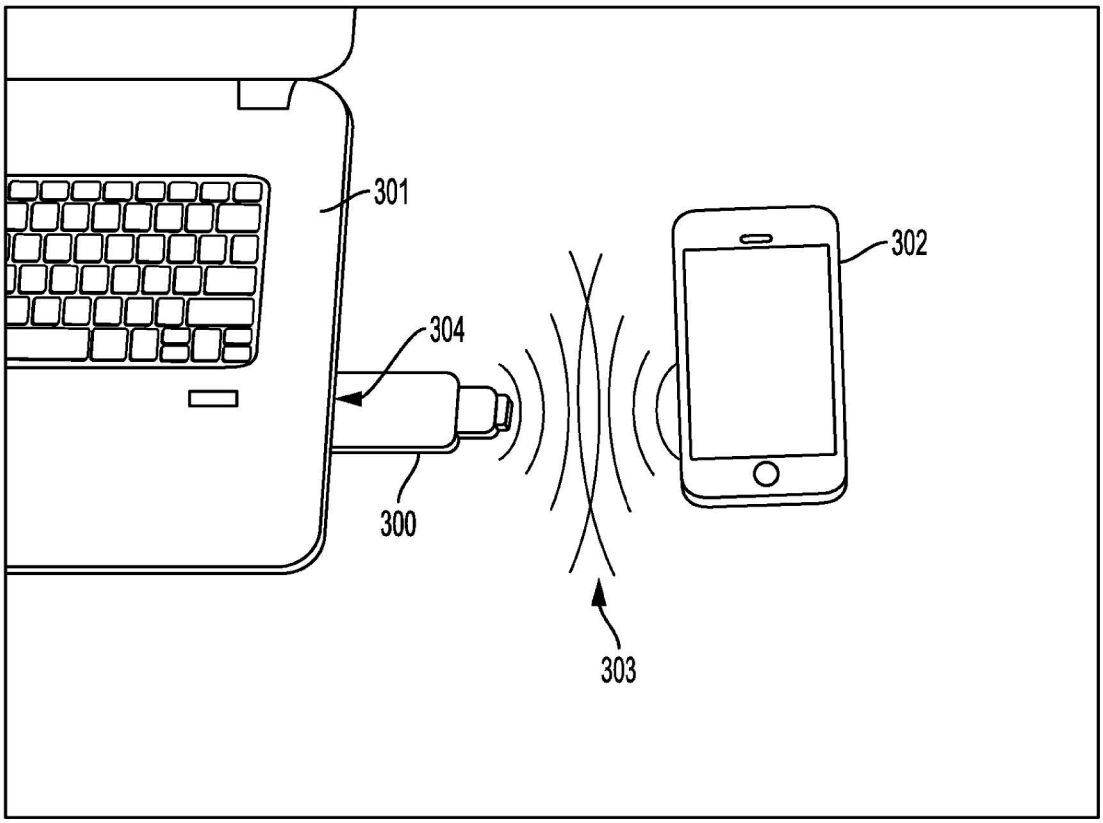
301
302
304
300
303

FIG. 3

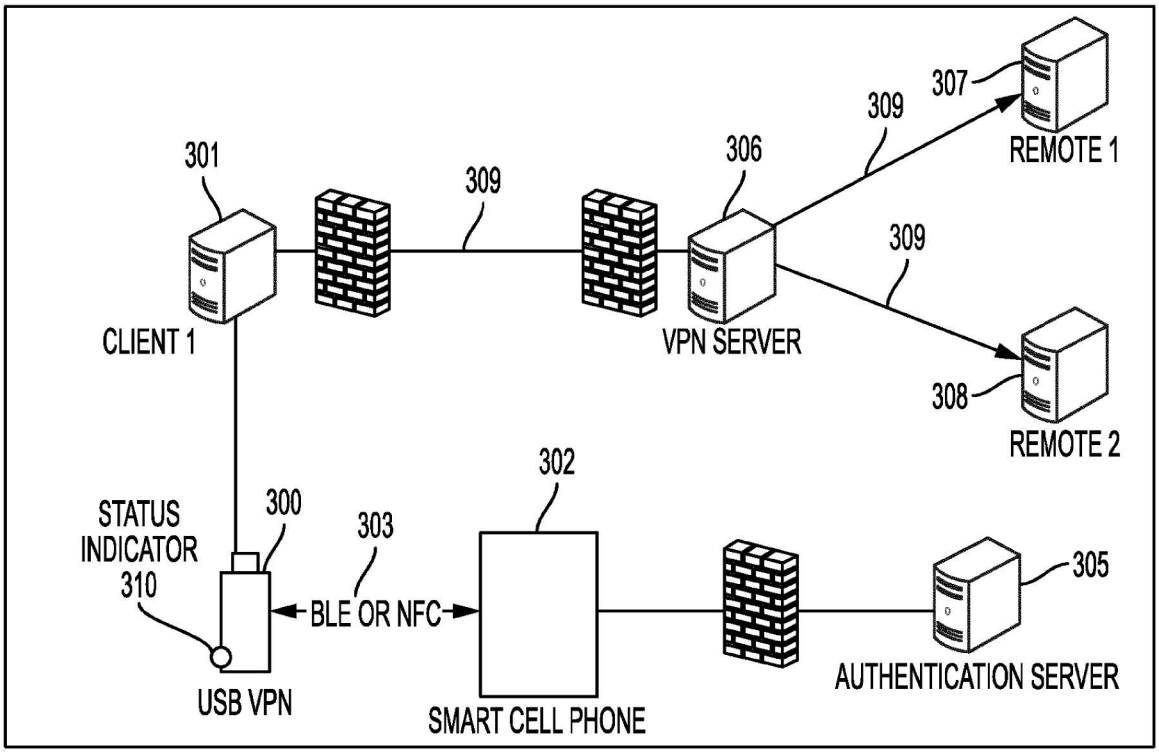
307
309
REMOTE 1
301
309
306
309
CLIENT 1
VPN SERVER
308
REMOTE 2
302
STATUS
INDICATOR
310
300
303
BLE OR NFC
305
AUTHENTICATION SERVER
USB VPN
SMART CELL PHONE

FIG. 4

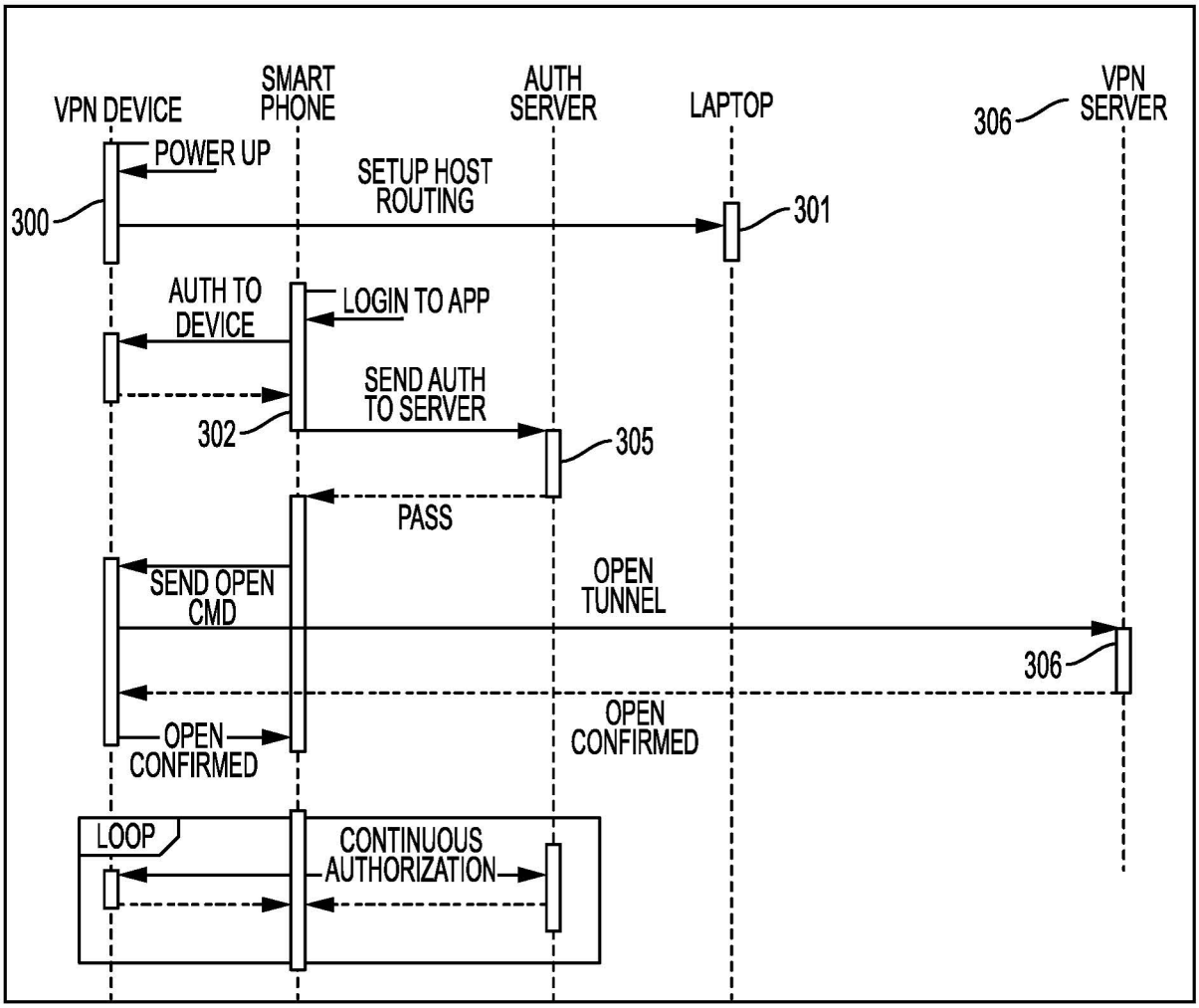
VPN DEVICE
SMART PHONE
AUTH SERVER
LAPTOP
306
VPN SERVER
POWER UP
300
SETUP HOST ROUTING
301
AUTH TO DEVICE
LOGIN TO APP
SEND AUTH TO SERVER
302
305
PASS
SEND OPEN CMD
OPEN TUNNEL
306
OPEN CONFIRMED
OPEN CONFIRMED
LOOP
CONTINUOUS AUTHORIZATION

FIG. 5

REFERENCES CITED IN THE DESCRIPTION

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

- US 20090319782 A1 **[0007]**
- US 20130091537 A1 **[0008]**