(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 685 755**

(51) Int. CI.:

G06F 21/57 (2013.01)
G06F 21/86 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.10.2010 PCT/FR2010/052143**

(87) Fecha y número de publicación internacional: **21.04.2011 WO11045516**

(96) Fecha de presentación y número de la solicitud europea: **11.10.2010 E 10782340 (3)**

(97) Fecha y número de publicación de la concesión europea: **30.05.2018 EP 2488984**

(54) Título: **Sistema informático de acceso a datos confidenciales por al menos una carcasa remota y carcasa remota**

(30) Prioridad:

12.10.2009 FR 0957127

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.10.2018

(73) Titular/es:

GROUPE DES ECOLES NATIONALES D'ECONOMIE ET STATISTIQUE (100.0%)
5 avenue Henry le Chatelier
91120 Palaiseau, FR

(72) Inventor/es:

GADOUCHE, KAMEL y
DEBONNEL, ERIC

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Sistema informático de acceso a datos confidenciales por al menos una carcasa remota y carcasa remota

La presente invención se refiere a un sistema informático de acceso a datos confidenciales por al menos una carcasa remota así como a una carcasa remota. Tiene aplicaciones en el ámbito del tratamiento de la información, más particularmente para la seguridad de datos confidenciales contenidos en un medio informatizado centralizado y que deben tratarse por usuarios remotos de dicho medio informatizado centralizado.

La invención objeto de esta solicitud se ha desarrollado en el Grupo de las Escuelas Nacionales de Economía y Estadística de Francia (GENES, *Groupe des Ecoles Nationales d'Economie et Statistique*) relacionado con el Instituto Nacional de la Estadística y de los Estudios Económicos de Francia (INSEE, *Institut National de la Statistique et des Etudes Economiques*) relacionado con el Ministerio de Economía, Industria y Empleo francés.

En muchas industrias, comercios o establecimientos públicos de educación y/o investigación, existen bases de datos informáticas que contienen informaciones sensibles que deben permanecer confidenciales o, al menos, que no se deben poder transferir o copiar fuera del sitio en el que están almacenadas y tratadas, en general en un servidor informático. Sin embargo, puede ser necesario para usuarios exteriores al sitio de almacenamiento y por la mediación de una red informática pública, en particular INTERNET®, poder usar estas informaciones que son por ejemplo datos individualizados para efectuar cálculos, búsquedas, etc. con el fin de producir resultados a partir de estos datos confidenciales, resultados que no deben permitir llegar a los datos individuales de partida.

Es deseable por tanto disponer de un sistema que permita el acceso y el tratamiento de estos datos confidenciales sin por ello que el usuario o incluso un tercero malicioso pueda recuperar, a partir de un acceso a distancia, los datos confidenciales contenidos en un servidor centralizado.

Es deseable igualmente que la arquitectura del sistema propuesto pueda responder en buenas condiciones a las necesidades de los usuarios/buscadores que quieren trabajar sobre estos datos sensibles/confidenciales. Es por tanto necesario tomar en consideración muchos imperativos, como unos imperativos de seguridad elevada sobre todos los componentes de la arquitectura, unos imperativos de ergonomía de los que en concreto una interfaz y unas herramientas para los usuarios/buscadores que les permiten trabajar en buenas condiciones, unos imperativos de integración porque hay que poder integrarse en el entorno informático de los establecimientos remotos de los usuarios/buscadores cualquiera que sea, y unos imperativos económicos.

En la práctica, el objetivo de seguridad del acceso a datos sensibles/confidenciales se alcanza gracias a la combinación de medios materiales y de medios de software, en concreto una carcasa remota especialmente configurada y en concreto una conexión túnel cifrada en una red pública. Se propone en este documento, para acceder a datos confidenciales, la implementación de un equipo particular en una estación remota que es una “caja negra” dedicada y bloqueada en el seno de una arquitectura material y de software particular.

Por el otro lado, el estado de la técnica en el campo de aplicación contemplado se basa en soluciones meramente de software. Ahora bien, una solución meramente de software no responde a la problemática expuesta:

- Es menos segura porque se basa en un soporte no dominado que es la estación de trabajo del usuario remoto (ETUR). Este sistema se expone entonces a una fuga de los datos accidental o intencional (software espía, sistema de captura de pantalla con reconocimiento de caracteres...)
- Es más costosa en términos de despliegue porque la ETUR no es forzosamente compatible, en términos de mantenimiento porque la evolución de la ETUR impone un redespliegue e inversamente la evolución de la solución de software puede solicitar una actualización de la ETUR, en términos de asistencia porque una modificación de la ETUR puede generar fallos de la solución de software, etc.

Es esta unión con el entorno informático del usuario remoto la que explica que una solución meramente de software no responda a las necesidades expuestas. La invención propone por tanto un sistema que implementa unos medios materiales que permiten librarse de los inconvenientes mencionados anteriormente.

Se conoce en el ámbito del control de acceso el sistema descrito en el documento US 2007/245409 A1 en el que se implementan un cliente 10 y un servidor de ficheros 30 conectados por una conexión HTTPS y el cliente incluye aplicaciones. Esta conexión puede ser directa o no, por la mediación de un dispositivo intermedio 1250 (“appliance” o “proxy server”). Se prevé que este dispositivo 1250 incluya un procesador de encriptación 3260. En este documento, la máquina local (cliente) es un aparato cualquiera, por ejemplo un microordenador clásico dotado de los softwares y sistema operativo habituales. Se indica en concreto en el mismo que la máquina local (cliente) puede solicitar una aplicación y datos al servidor y, como respuesta, el servidor le envía la aplicación y los datos para ejecución local. La máquina local de este documento puede incluir unos medios de almacenamiento amovibles (ej.: CD-R/RW, “USB storage devices”) que permiten por tanto el registro de datos localmente y su difusión o la carga de programas en la máquina local.

El documento EP 1 962 221 A1 divulga un “OS” en memoria de solo lectura y encriptado. Durante la inicialización del BIOS el mismo se desencripta para que sea operacional.

El documento US 2002/042 882 A1 divulga un cierto número de funciones y/o dispositivos destinados a asegurar un nivel de seguridad elevado a un ordenador. Contra las intrusiones físicas, se propone un circuito de detección de falsificación así como un medio de identificación del usuario.

La invención se refiere por tanto a un sistema informático de acceso a datos confidenciales por al menos una carcasa remota usada por un usuario, estando los datos almacenados en un medio informático centralizado seguro que incluye un medio de tratamiento de dichos datos destinado a producir resultados, estando una conexión informática establecida entre dicha carcasa remota y el medio informático centralizado, siendo la carcasa remota un microordenador que funciona bajo la dependencia de un sistema operativo local que arranca con una fase de inicio.

Según la invención, el sistema está configurado de tal manera que la conexión informática es una conexión túnel cifrada en una red pública que está establecida en el seno del sistema de modo que la carcasa remota esté integrada lógicamente en el medio informático centralizado con el fin de que dicha carcasa remota sea administrable únicamente a distancia y de modo que dicha carcasa no sea explotable en ausencia del establecimiento de la conexión informática, estando el sistema configurado además de tal manera que durante los accesos a los datos dicha carcasa remota solo reciba informaciones de visualización relacionadas con el tratamiento efectuado sobre los datos y producidas por el medio informático centralizado, teniendo el microordenador de la estación remota la forma de una tarjeta electrónica que incluye además un circuito electrónico de encriptación, el sistema operativo así como las informaciones necesarias para el funcionamiento de dicha carcasa remota que están almacenados de manera encriptada en dicha carcasa remota, y dicha carcasa remota está constituida por una carcasa sellada que contiene la tarjeta electrónica y entradas/salidas de las que una entrada/salida de medio(s) de identificación/identificaciones conectada a al menos un medio de identificación del usuario y una entrada/salida de red informática destinada a la conexión túnel cifrada.

El término microordenador para la carcasa remota cubre en realidad cualquier dispositivo de programable que permita un acceso red y que incluya unos medios de interfaz con un usuario.

En diversos modos de implementación de la invención, se emplean los medios siguientes que pueden usarse solos o según todas las combinaciones técnicamente posibles:

- la carcasa remota es únicamente administrable a distancia por el medio informático centralizado,
- carcasa remota incluye además un medio de configuración local accesible y visible por el usuario, incluyendo dicho medio de configuración local un visualizador y un conjunto de teclas dispuestos en la carcasa y que permiten una configuración en el sitio de parámetros locales,
- los parámetros locales configurables son por ejemplo configuraciones de visualización, la dirección red de la carcasa,
- la red pública es una red INTERNET®,
- la carcasa remota incluye un número reducido de entradas/salidas físicas conectables,
- las entradas/salidas físicas conectables son una entrada/salida de teclado, una entrada/salida para órgano de tipo puntero, por ejemplo ratón, una entrada/salida de medio(s) de identificación/identificaciones, una entrada/salida de pantalla de visualización, una entrada/salida de red informática destinada a la conexión túnel cifrada,
- el circuito electrónico de encriptación de la tarjeta electrónica de la carcasa es del tipo TPM (“Trusted Platform Module”),
- el circuito electrónico de encriptación TPM funciona con la tecnología BitLocker®,
- la tarjeta electrónica microordenador incluye un BIOS bloqueable con contraseña,
- la tarjeta electrónica microrordenador presenta una o varias de las características siguientes: capacidad memoria central al menos 2 Go, visualización gráfica tipo VGA y/o DVI, entrada/salida de red informática al menos 10/100 Mbits/s, dos entradas/salidas de tipo USB, memoria de masa de al menos 32 Go (chip o mecánica),
- la entrada/salida de red informática está sobre conector RJ45,
- la entrada/salida de red informática es compatible con un inicio PXE (“Pre-boot eXecution Environment”: arranque por la red) parametrizable y activable/desactivable a partir del BIOS de la tarjeta electrónica,
- la tarjeta electrónica se basa en una tarjeta PC industrial de formato reducido,
- la tarjeta electrónica de la carcasa remota es de tipo Mini-ITX,
- la carcasa remota mide aproximadamente H 70 mm x P 200 mm x L 240 mm,
- la conexión túnel cifrada en una red pública se efectúa indirectamente a partir de la carcasa remota, estando la carcasa remota conectada a una red local y estando un equipo de interconexión a la red pública conectado a dicha red local,
- la conexión túnel cifrada en una red pública se efectúa directamente a partir de la carcasa remota, o bien un equipo de interconexión a la red pública está dispuesto entre la entrada/salida de red informática de la carcasa remota y la red pública, o bien el equipo de interconexión a la red pública está incorporado a la carcasa remota,
- el equipo de interconexión a la red pública está incorporado a la carcasa remota y se omite la entrada/salida de red informática de la carcasa remota,

- el equipo de interconexión a la red pública está incorporado a la carcasa remota y la entrada/salida de red informática de la carcasa remota está presente, lo que permite usar la carcasa remota en directo o indirecto en la red pública,
- el equipo de interconexión a la red pública es del tipo alámbrico o radio,
- la conexión túnel cifrada es del tipo VPN-SSL (“Secure Sockets Layer virtual private network”),
- el cifrado sobre la conexión túnel cifrada es doble, de los tipos SSTP (“Secure Socket Tunneling Protocol”), RDP (“Remote Desktop Protocol”),
- el sistema operativo de la estación remota se selecciona entre los productos de la familia WINDOWS®,
- la carcasa remota incluye además un cortafuegos, que la protege de la red local anfitrión,
- el visualizador incluye un visualizador alfanumérico con cristales líquidos,
- el visualizador alfanumérico con cristales líquidos es del tipo 1 línea 16 caracteres,
- el visualizador alfanumérico con cristales líquidos es del tipo 2 líneas 16 caracteres,
- el conjunto de teclas es un conjunto reducido de menos de 7 teclas,
- la carcasa remota se alimenta eléctricamente por una fuente de alimentación exterior a la carcasa,
- la fuente de alimentación exterior a la carcasa es una alimentación sector,
- el medio informático centralizado incluye además un cortafuegos en la conexión túnel cifrada,
- el cortafuegos prohíbe cualquier conexión saliente del medio informático centralizado,
- el medio informático centralizado incluye un servidor SSTP (“Secure Socket Tunneling Protocol”) de conexión túnel SSL (“Secure Sockets Layer”), al menos un servidor de tratamiento que incluye los datos confidenciales, un servidor de administración de la seguridad, estando dichos servidores del medio informático centralizado en una red local dedicada,
- el medio informático centralizado incluye además un servidor de copia de seguridad disco en la red local dedicada,
- dichos servidores del medio informático centralizado son físicamente uno o varios aparatos informáticos, en efecto, las funciones de los servidores distintos pueden separarse o agruparse en uno o varios aparatos informáticos del tipo ordenador físico, microordenador físico, servidor físico,
- el servidor de gestión de la seguridad es administrador de certificados, controlador de dominio, de la política de seguridad de la(s) carcasa(s) remota(s), de su supervisión y su repudio,
- los medios de identificaciones se eligen entre uno o varios de los medios siguientes: un lector de tarjeta chip, un lector biométrico, un lector de huella numérica,
- un medio de identificación es una contraseña.

La invención se refiere igualmente a una carcasa remota para implementación en un sistema informático de acceso a datos confidenciales por al menos una carcasa remota usada por un usuario, estando los datos almacenados en un medio informático centralizado seguro que incluye un medio de tratamiento de dichos datos destinado a producir resultados, estando una conexión informática establecida entre dicha carcasa remota y el medio informático centralizado, siendo la carcasa remota un microordenador que funciona bajo la dependencia de un sistema operativo local que arranca con una fase de inicio, teniendo dicha carcasa una o varias de las características descritas y en concreto siendo de tal forma que está adaptada especialmente al sistema de la invención y que permite que la conexión informática sea una conexión túnel cifrada en una red pública y que dicha carcasa no sea explotable en ausencia del establecimiento de la conexión informática, permitiendo la conexión túnel cifrada la integración lógica de la carcasa remota en el medio informático centralizado con el fin de que dicha carcasa remota sea administrable únicamente a distancia, teniendo el microordenador de la estación remota la forma de una tarjeta electrónica que incluye además un circuito electrónico de encriptación, estando el sistema operativo así como las informaciones necesarias para el funcionamiento de dicha carcasa remota almacenados de manera encriptada en dicha carcasa remota, y dicha carcasa remota está constituida por una carcasa sellada que contiene la tarjeta electrónica y entradas/salidas de las que una entrada/salida de medio(s) de identificación/informaciones conectada a al menos un medio de identificación del usuario y una entrada/salida de red informática destinada a la conexión túnel cifrada.

La invención se comprenderá mejor, gracias a la descripción de a continuación, que está relacionada con un modo de realización preferido, dado a título de ejemplo no limitativo, y explicado con referencia al dibujo adjunto, en el que la figura 1 es una representación esquemática de la arquitectura general del sistema.

En el ejemplo de realización descrito a continuación, se considera el caso de un entorno de búsqueda en el que el usuario es un buscador que debe acceder a distancia a los datos confidenciales almacenados en un centro seguro que incluye un servidor de dichos datos. En este contexto, la carcasa remota constituye un terminal sobre el que el buscador trabaja.

Esta carcasa remota, que tiene la forma de una carcasa de tamaño reducido que incluye una tarjeta electrónica de microordenador, está segura física y funcionalmente contra usos no conformes y no autorizados. Estos medios de seguridad son en concreto bloqueos físicos y/o lógicos de los puertos externos no previstos para la explotación del sistema. Por ejemplo un eventual puerto serie RS232 o paralelo de la tarjeta electrónica no está conectado a su conector o el conector está ausente o está escondido/se hace no utilizable. Cabe señalar que como cualquier entrada/salida del microordenador, el bloqueo puede ser igualmente lógico/de software: el/los puertos en cuestión no tiene(n) piloto(s) en el sistema operativo de la carcasa remota o el piloto está desactivado. Igualmente, la carcasa está protegida físicamente contra las intrusiones por su estructura (resistencia mecánica, ausencia de abertura en

ciertas partes de la carcasa...), su modo de ensamblado (uso de tornillo de seguridad), detección de intrusión por un contactor eléctrico, por una célula fotoeléctrica...

Por otro lado, para el establecimiento de la conexión túnel cifrada entre la carcasa remota del usuario y el centro seguro con su servidor de datos, la secuencia de inicio está preestablecida mediante programación anterior de la estación remota. Además, el sistema operativo local está bloqueado y las informaciones memorizadas en la carcasa de la estación remota, programas o datos locales, lo están en forma encriptadas.

La estación remota es por tanto una carcasa autónoma restringida que abarca su propio sistema operativo (Windows Vista® en este ejemplo). Esta carcasa está protegida de la red local anfitrión por un cortafuegos abarcado y sus puertos USB® están restringidos a los periféricos autorizados mediante software gracias al dispositivo de administración centralizado que se pone en marcha al inicio de la carcasa.

Para usar su carcasa remota, el buscador debe abrir en ella una sesión, lo que solo puede hacerse autenticándose con la ayuda de un medio de identificación que es en este documento una tarjeta chip que contiene un certificado válido, acceso por código pin, y que se lee por un lector conectado a la estación por una conexión USB. En un modo preferido de realización, un sensor biométrico se implementa igualmente para la autenticación del buscador, preferentemente del tipo lector de huella digital.

De manera general, en lo relativo a los usuarios, una formación adecuada de los usuarios en lo relativo al sistema es preferible y la primera conexión de la estación remota se efectúa preferentemente bajo el control del administrador del sistema lo que permite una inicialización del código pin de la tarjeta chip y la toma de las huellas en caso de que se implemente un sensor de este tipo.

Una vez abierta la sesión en la estación remota, un programa de acceso al servidor de datos confidenciales del medio informático centralizado seguro se ejecuta con el fin de crear la conexión informática túnel cifrada en una red pública, por ejemplo INTERNET®, y es el único programa que puede ejecutarse después de una apertura de sesión. En consecuencia, el usuario solo ve y solo puede usar un solo programa predefinido con antelación. Un utilitario de software de la carcasa remota vigila la actividad del buscador (pulsaciones de teclas en concreto) y cuando detecta una ausencia de actividad durante un tiempo determinado (un contador de tiempo de inactividad que aumenta automáticamente se pone a cero en cada acción del buscador), cierra la sesión que estaba abierta y/o da la posibilidad durante un tiempo determinado al buscador de efectuar una acción que vuelve a poner a cero el contador de tiempo de inactividad. De este modo, si el buscador olvida cerrar su sesión al final de su trabajo, lo será automáticamente lo que limitará los riesgos de uso de la estación remota por una tercera persona una vez marchado el buscador. En un modo preferido de realización, un utilitario particular solicitará al usuario de la carcasa remota una autenticación biométrica con intervalo de tiempo regular. Ello con el fin de asegurarse de manera permanente de la verdadera identidad del usuario.

Para la creación de la conexión túnel cifrada, todos los elementos de información que permitan la conexión red están disponibles y cifrados en la memoria de masa de la estación remota. En efecto, la tarjeta electrónica de microordenador, llamada placa madre, de la carcasa remota incluye un chip de encriptación y la/las claves de encriptación usadas están almacenadas en la carcasa remota igualmente de una manera encriptada. Por construcción, ningún dato confidencial del medio informático centralizado seguro se transfiere y almacena en la estación remota, solo copias de pantalla o instrucciones de visualización se envían a la estación remota por el servidor seguro central que contiene los datos confidenciales. Todos los intercambios entre la estación remota y el servidor seguro central se hacen por la red pública, INTERNET® en este ejemplo, y se han puesto en marcha un sistema de comunicación cifrado, un túnel cifrado, de extremo a extremo. Por otro lado, solo las carcasas remotas que se encuentran físicamente en establecimientos identificados por su dirección red pueden alcanzar, en el medio informático centralizado seguro, el servidor seguro central que contiene los datos confidenciales.

Aun por razones de seguridad, el sistema se ha concebido para permitir realizar a distancia todas las operaciones de gestión, de vigilancia, de actualización de software y seguridad de cada estación remota. Igualmente, permite poder autorizar o repudiar centralmente (lado del medio informático centralizado seguro) una estación remota o un certificado dado.

La carcasa remota puede integrarse en cualquier entorno informático y de red local del sitio del usuario/buscador. Por ello, es preferible que la configuración de este entorno informático y esta red local se conozca para administrar eficazmente la seguridad de los accesos por el medio informático centralizado seguro que incluye el servidor de datos confidenciales.

La conexión entre la estación remota y el medio informático centralizado seguro se hace en dos pasos. En un primer paso, lado carcasa remota, la inserción de la tarjeta chip en el lector de tarjeta y acoplado con la identificación biométrica (huella) y una contraseña, permiten abrir una sesión local en la estación remota. Una vez abierta, la sesión local permite al buscador, en un segundo paso, conectarse al medio informático centralizado seguro y abrir en el mismo una sesión central (por ejemplo usando la misma contraseña). La identificación permitida por la tarjeta chip es necesaria para la apertura de las dos sesiones. Cabe señalar que el hecho de retirar la tarjeta del lector solo

cierra la sesión local, dejando la sesión central activa, se la encuentra en el estado en el que se le ha dejado al volver a abrir la sesión local en la estación remota, es decir al volver a poner la tarjeta chip en el lector y la identificación biométrica y al volver a dar la contraseña. Para desconectarse de la sesión central, basta con cerrarla. Cabe señalar que como para la estación remota, como opción, una detección de inactividad al nivel del medio informático centralizado seguro puede implementarse para cerrar al cabo de un tiempo determinado cualquier sesión arrancada por una estación remota y en la que ninguna actividad ha tenido lugar en el medio informático centralizado.

Se acaba de ver por tanto lo referente a la estación remota que los usuarios usan para acceder a los datos confidenciales. Se va a ver ahora lo referente al medio informático centralizado seguro que almacena los datos confidenciales y que incluye unos medios de tratamiento de dichos datos.

El medio informático centralizado seguro incluye un servidor seguro sobre el que los buscadores se conectan a distancia para trabajar. Típicamente, este servidor posee cuatro procesadores, 28 Go de memoria viva, 1,7 To de disco duro ultrarrápido. Es por otra parte en gran medida evolutivo (posibilidad de adición de memoria y de procesadores en caso necesario y agrupación/“clúster”). Dispone de una interfaz Windows® con los softwares habitualmente usados en materia de tratamiento de datos estadísticos.

Con el fin de mejorar aun más la seguridad, un usuario se define por el par [identificador, proyecto] lo que tiene como consecuencia que un mismo buscador que trabaja sobre dos proyectos no tendrá acceso a los datos de los dos proyectos durante la misma sesión. Asimismo, los espacios de trabajo que contienen los ficheros de datos de cada proyecto están aislados los unos de los otros. Por una parte, los permisos de acceso para cada proyecto están perfectamente definidos. Y, por otra parte, es imperativo evitar la compartición de información y/o de recursos (datos, programas...) para garantizar, por ejemplo, que ninguna tabla temporal de un proyecto pueda accederse por los miembros de otro proyecto.

Aun en el medio informático centralizado seguro, un servidor de copia de seguridad permite guardar sobre disco todas las configuraciones sistema y todos los trabajos de los buscadores. Cabe señalar que la solución de copia de seguridad a base de bandas magnéticas no se ha seleccionado para evitar cualquier difusión de estas bandas y de los datos que contienen.

Cabe señalar igualmente que para mejorar aun más la seguridad, cualquier entrada y/o salida relativa a datos confidenciales en el medio informático centralizado seguro solo puede/pueden hacerse manualmente mediante desplazamiento físico de un operador en el sitio e, incluso preferentemente, en el local seguro que contiene el medio informático centralizado seguro. De manera general, cualquier entrada de información (datos de cualquier formato, programas en forma de fuente...) en el medio informático centralizado seguro se efectúa bajo el control de un administrador del sistema.

Típicamente, los usuarios/buscadores tienen acceso:

- a los datos confidenciales a los que deben tener acceso en el marco de su proyecto y que están almacenados en un directorio específico (“SA-Sources”).
- a un espacio destinado a alojar los ficheros intermedios creados en el marco de sus proyectos: programas, bases de datos, textos, etc. Este espacio es accesible en el interior de un directorio específico (“EA-Projets”) y más particularmente en una carpeta cuyo nombre es el “nombre corto” del proyecto de búsqueda y que figura en su tarjeta chip. En el interior de esta carpeta, cada buscador que participa en el proyecto dispone de una subcarpeta cuyo nombre es su propio “nombre corto” de buscador.

Los proyectos están por tanto compartimentados. Los buscadores relacionados con otros proyectos no pueden acceder a ninguno de los subespacios correspondientes y los buscadores que trabajan juntos en un proyecto no pueden acceder a los subespacios personales de cada uno, sino que acceden todos al directorio raíz de su proyecto en el que pueden poner ficheros y crear directorios compartidos. Los administradores de datos no tienen tampoco acceso a los espacios de trabajo de los buscadores. Los buscadores pueden trabajar en el interior del medio informático centralizado seguro a partir de sus estaciones remotas, usando estos espacios, estos ficheros y los softwares disponibles. No obstante, los buscadores no pueden exportar nada de manera autónoma, ni sobre una impresora, ni sobre un fichero externo y no pueden tampoco hacer “copiar/cortar/pegar”.

De este modo, los buscadores solo pueden exportar resultados que respetan el secreto estadístico, es decir resultados que no permiten el acceso a los datos confidenciales individuales y no pueden exportar por tanto informaciones de identificación, directa o indirecta, por ejemplo, de una persona o de una empresa y que están almacenados en el servidor central.

En un modo de implementación particular, el dispositivo de exportación está configurado de la manera siguiente:

- Los buscadores constituyen en su espacio personal “el objeto” que desean exportar en un fichero, asegurándose que respeta perfectamente el secreto estadístico y complementan este objeto con una corta documentación que

lo describe en otro fichero.

- Los buscadores depositan estos dos ficheros en un directorio de “salida” que es no accesible en lectura para los buscadores, en el modelo de una urna: el depósito es posible, pero no la consulta ni la modificación una vez efectuado el depósito.
- Los buscadores envían un mensaje a un servicio de administración de los datos del sistema señalando la solicitud de salida. Un administrador de los datos del sistema examina entonces los “objetos” contenidos en dicho directorio de salida. Si los datos están bien conformes con el secreto estadístico, los transfiere en un directorio de “Partida” que es no accesibles para los buscadores y una copia de “el objeto” se archiva al mismo tiempo.
- Unos informáticos transfieren físicamente los “objetos” del directorio “Partida” en una cuenta que se encuentra fuera del medio informático centralizado seguro y una vez efectuada esta operación, estos “objetos” se envían por mensajería electrónica a sus destinatarios.

En lo referente a las informaciones que pueden importarse en el medio informático centralizado seguro por los usuarios, solo pueden importarse objetos “inactivos/no ejecutables” (ninguno ejecutable) o programas de un tipo dado documentados. La importación se efectúa bajo el control de un administrador a quien los buscadores envían por mensajería electrónica “el objeto” en cuestión así como una descripción de cada fichero. Tras control, el investigador es informado de la importación y encuentra sus ficheros en un directorio específico del medio informático centralizado seguro al que tiene acceso.

La Figura 1 presenta la arquitectura general del sistema. A la izquierda de la Figura 1 se ha representado lo referente al usuario con su estación remota 1 que incluye la carcasa remota 4 a la que está conectado por conexión USB® un teclado (no representado), unos lectores 6 de tarjeta chip y biométrica así como una pantalla de visualización 5. Un medio de apuntamiento (no representado) puede estar conectado igualmente por conexión USB® a la carcasa. La carcasa 4 solo contiene un sistema operativo VISTA® bloqueado y todas las informaciones de conexión están cifradas. Esta carcasa 4 está conectada a una red local 7 tipo ETHERNET® conectada a un equipo terminal 8 de conexión a una red INTERNET® 2. De este modo, en este ejemplo, la conexión túnel cifrada en INTERNET® se efectúa indirectamente a partir de la carcasa, teniendo la entrada/salida de red informática de la estación remota que está conectada a una red local un acceso a la red INTERNET®. El establecimiento en el que está dispuesta la estación remota 1 posee una dirección IP. Sobre la red INTERNET® 2, entre el medio informático centralizado seguro y la estación remota, nada transita en claro y todo está cifrado doblemente (SSTP, RDP) en un túnel cifrado.

En la parte derecha de la Figura 1 se ha representado lo referente al medio informático centralizado seguro 3 en el que están almacenados los datos confidenciales. Un cortafuegos 9 está dispuesto en interfaz del medio informático centralizado seguro sobre la red INTERNET® 2 en la que está establecida una conexión túnel cifrada VPN SSL entre la estación remota y el medio informático centralizado seguro 3. Este último incluye un servidor de aplicación 11 SECHPC01 que permite el almacenamiento y el tratamiento seguro de los datos confidenciales, un servidor de gestión de la seguridad 12, un servidor de copia de seguridad DPM 2007 y un servidor de comunicación SSTP para el túnel SSL. Este conjunto de servidores está en una red local dedicada en el seno del establecimiento en el que se encuentra el medio informático centralizado seguro 3. En esta red local dedicada, las introducciones/extracciones (entradas/salidas) de datos confidenciales solo pueden ser, preferentemente, manuales por un operador. El cortafuegos 9 solo autoriza las entradas de flujo cifrados procedentes de los establecimientos declarados y autorizados poseedores de carcasas remotas. Ninguna conexión saliente está autorizada y solo copias de pantalla o instrucciones de visualización se vuelven a enviar del medio informático centralizado seguro hacia las carcasas remotas. Ningún dato confidencial puede salir del medio informático centralizado seguro 3.

Se comprende bien que la invención puede declinarse según muchas otras posibilidades sin por ello salirse del ámbito definido por las reivindicaciones. Finalmente, las denominaciones protegidas mencionadas en este documento pertenecen a sus propietarios.

REIVINDICACIONES

1. Carcasa remota para implementación en un sistema informático de acceso seguro a datos confidenciales por al menos una carcasa remota (4) usada por un usuario y específica y únicamente concebida para este acceso seguro, estando los datos almacenados en un medio informático centralizado seguro (3) que incluye un medio de tratamiento de dichos datos destinado a producir resultados, estando una conexión informática (2) túnel cifrada en una red pública establecida entre dicha carcasa remota y el medio informático centralizado, siendo la carcasa remota un microordenador que funciona bajo la dependencia de un sistema operativo local que arranca con una fase de inicio, estando el sistema configurado de tal manera que durante los accesos a los datos dicha carcasa remota solo reciba informaciones de visualización relacionadas con el tratamiento efectuado sobre los datos y producidas por el medio informático centralizado, no transmitiéndose por tanto los datos del medio informático centralizado a la carcasa, teniendo el microordenador de la carcasa remota la forma de una tarjeta electrónica que incluye entradas/salidas y un circuito electrónico de encriptación,
caracterizada por que dicha carcasa remota está constituida por una carcasa sellada y **por que**

- la tarjeta electrónica incluye:

  ◦ una entrada/salida destinada a un(os) medio(s) de identificación/identificaciones (6) conectada a al menos un medio de identificación del usuario y
  ◦ una entrada/salida de red informática (7) destinada a la conexión túnel cifrada, y **por que**

- la carcasa remota (4) incluye unos medios de explotación que permiten:

  ◦ por una parte y bajo reserva de una autenticación del usuario, la apertura de una sesión local en dicha carcasa y la implementación de una fase de inicio con creación de la conexión informática túnel cifrada entre dicha carcasa remota y el medio informático centralizado, estando entonces la carcasa remota integrada lógicamente en el medio informático centralizado, y permitiendo su administración únicamente a distancia por el medio informático centralizado, y
  ◦ por otra parte, autorizando únicamente una configuración local de parámetros locales por un medio de configuración local que es accesible y visible por el usuario, incluyendo dicho medio de configuración local un visualizador y un conjunto de teclas dispuestas sobre la carcasa y que permiten una configuración de la dirección red de la carcasa,

- estando los medios de explotación y las informaciones necesarias para el funcionamiento de dicha carcasa remota almacenados de manera encriptada en dicha carcasa remota,

  ◦ estando la carcasa destinada a formar con el medio informático centralizado seguro un conjunto funcionalmente indisociable: solo pudiendo la carcasa conectarse al medio informático centralizado seguro y, recíprocamente, solo aceptando el medio informático centralizado seguro una conexión de dicha carcasa autenticada.

2. Carcasa remota según la reivindicación 1, **caracterizada por que** está configurada con el fin de que la conexión túnel cifrada en una red pública se efectúe indirectamente a partir de la carcasa remota, estando la carcasa remota conectada a una red local y estando un equipo de interconexión a la red pública conectado a dicha red local.

3. Carcasa remota según la reivindicación 1, **caracterizada por que** está configurada con el fin de que la conexión túnel cifrada en una red pública se efectúe directamente a partir de la carcasa remota, o bien un equipo de interconexión a la red pública está dispuesto entre la entrada/salida de red informática de la carcasa remota y la red pública, o bien el equipo de interconexión a la red pública está incorporado a la carcasa remota.

4. Carcasa remota según una cualquiera de las reivindicaciones anteriores, **caracterizada por que** el visualizador incluye un visualizador alfanumérico con cristales líquidos, siendo el conjunto de teclas un conjunto reducido de menos de 7 teclas.

5. Carcasa remota según una cualquiera de las reivindicaciones anteriores, **caracterizada por que** los medios de identificaciones se seleccionan entre uno o varios de los medios siguientes: un lector de tarjeta chip, un lector biométrico, un lector de huella digital.

6. Sistema informático de acceso seguro a datos confidenciales para la carcasa remota (4) según una cualquiera de las reivindicaciones anteriores, estando los datos almacenados en un medio informático centralizado seguro (3), constituyendo la carcasa y el medio informático centralizado seguro el sistema, **caracterizado por que** el medio informático centralizado incluye además un cortafuegos (9) en la conexión túnel cifrada.

7. Sistema según la reivindicación 6, **caracterizado por que** el medio informático centralizado incluye un servidor SSTP de conexión túnel SSL, al menos un servidor de aplicación que incluye los datos confidenciales, un servidor de administración de la seguridad, estando dichos servidores del medio informático centralizado en una red local

dedicada.

8. Sistema según la reivindicación 7, **caracterizado por que** el medio informático centralizado incluye además un servidor de copia de seguridad en la red local dedicada.

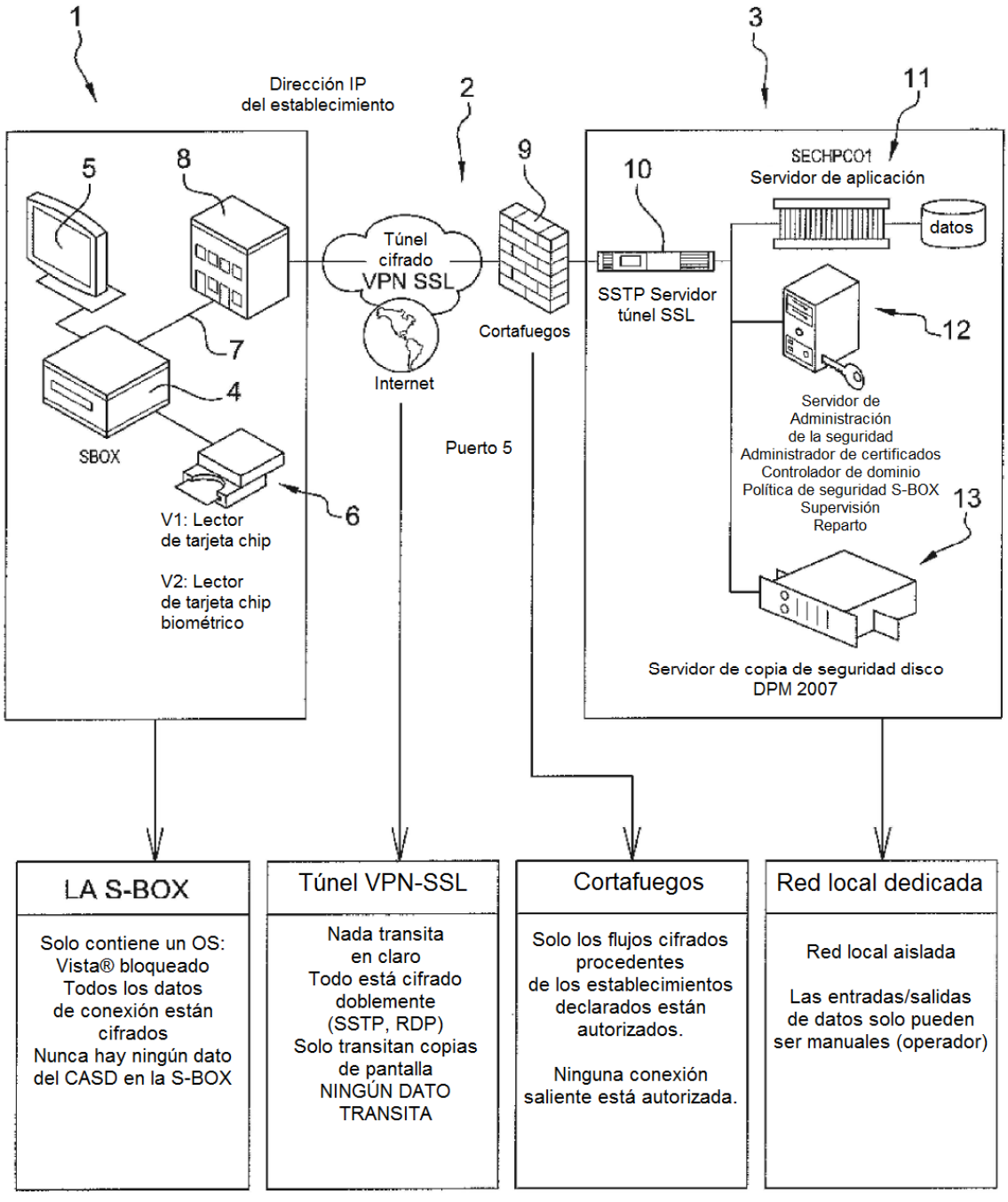
1
Dirección IP
del establecimiento
2
3
11
5
8
9
10
SECHPCO1
Servidor de aplicación
Túnel
cifrado
VPN SSL
datos
SSTP Servidor
túnel SSL
Cortafuegos
12
7
4
Internet
SBOX
Puerto 5
Servidor de
Administración
de la seguridad
Administrador de certificados
Controlador de dominio
Política de seguridad S-BOX
Supervisión
Reparto
13
6
V1: Lector
de tarjeta chip
V2: Lector
de tarjeta chip
biométrico
Servidor de copia de seguridad disco
DPM 2007
LA S-BOX
Solo contiene un OS:
Vista® bloqueado
Todos los datos
de conexión están
cifrados
Nunca hay ningún dato
del CASD en la S-BOX
Túnel VPN-SSL
Nada transita
en claro
Todo está cifrado
doblemente
(SSTP, RDP)
Solo transitan copias
de pantalla
NINGÚN DATO
TRANSITA
Cortafuegos
Solo los flujos cifrados
procedentes
de los establecimientos
declarados están
autorizados.
Ninguna conexión
saliente está autorizada.
Red local dedicada
Red local aislada
Las entradas/salidas
de datos solo pueden
ser manuales (operador)

Fig. 1