(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 638 553**

(51) Int. CI.:

G06F 21/57 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.12.2004 E 04368072 (7)**

(97) Fecha y número de publicación de la concesión europea: **26.07.2017 EP 1669833**

(54) Título: **Método para validar un sistema informático de confianza**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.10.2017

(73) Titular/es:

AMADEUS S.A.S. (100.0%)
485 Route du Pin Montard, Sophia Antipolis
06410 Biot, FR

(72) Inventor/es:

FRENKIEL, MICHEL y
MATHIEU, ERIC

(74) Agente/Representante:

ELZABURU, S.L.P

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método para validar un sistema informático de confianza

Campo técnico de la invención

La invención se refiere a telecomunicaciones de Manejo de Información y, más particularmente, a un proceso y aparato para asegurar el acceso a un Sistema de Manejo de Información (IHS).

Antecedentes de la técnica

El progreso constante de los sistemas y la tecnología de comunicación y la de los sistemas de comunicación, particularmente con la explosión de las redes de Internet e intranet, ha dado como resultado el desarrollo de una era de información y servicios. Hoy en día, los ordenadores y de manera más general los Sistemas de Manejo de Información (I.H.S.), tales como los ordenadores de sobremesa, los ordenadores portátiles y cualquier tipo de sistemas de mano o portátiles, se pueden usar para acceder a una amplia variedad de transacciones o servicios, donde quiera que esté el usuario o el cliente de la nueva era de información.

Esto plantea claramente el problema de la seguridad del acceso a la fuente de información y, de manera más general, a la transacción y los servicios.

En el nuevo mundo de la información, ejemplificado por el desarrollo de las redes de Internet e intranet, las cuestiones de seguridad se muestran que son cada vez más críticas.

Algunas técnicas ya son conocidas para resolver -al menos en parte- el problema de la seguridad de acceso a las bases de datos sensibles y, de manera más general, a cualquier Sistema de Manejo de Información.

Una de las primeras técnicas que se usó fue la combinación del id de usuario y contraseña bien conocidos que garantiza -hasta cierto punto- que un usuario que intenta acceder a un sistema predeterminado es un usuario autorizado. Cualquier usuario que no tenga ni id de usuario ni la contraseña correspondiente se considerará como un usuario no autorizado y se denegará el acceso al recurso. Aunque tal sistema ha demostrado una gran eficiencia en el pasado, ahora demuestra ser claramente insuficiente en los sistemas más recientes.

La combinación del identificador de usuario y la contraseña se mejoró mediante el uso de un lector de tarjetas inteligentes específico. De una forma más sofisticada, el procedimiento de inicio de sesión se sustituye (o completa) por el uso simultáneo de un lector de tarjetas inteligentes seguras con el fin de permitir a un sistema remoto asegurarse de que el supuesto usuario es el que posee de la tarjeta inteligente de autenticación. Claramente tal solución es una mejora significativa llevada a la seguridad del sistema, pero no evita ninguna modificación o ajuste no autorizado a la configuración del sistema que solicita acceso al servicio.

Se desarrollaron sistemas más sofisticados, basados en el uso de identificación biométrica o incluso la comprobación de algunos parámetros internos a la configuración del usuario, tales como la dirección del Protocolo de Internet (I.P.) del domicilio u oficina del cliente cuando este último intenta una conexión a un sistema remoto. Tales sistemas proporcionan soluciones parciales a algún problema de seguridad, pero no proporcionan una solución global que se pueda usar para una amplia variedad de sistemas IHS, basados en una configuración múltiple, que abarca tanto los datos de usuario como la configuración interna del sistema.

Ninguna solución garantiza que el sistema no haya sido modificado. Las modificaciones simples, como la adición de dispositivos tales como almacenamiento de datos USB o la sustitución de un lector biométrico por otro dispositivo, pueden ser perjudiciales, ya que permiten evitar la seguridad de las aplicaciones.

El documento EP-A-1 182 534 describe un método y un aparato para establecer confianza entre un usuario y una vista de ordenador como una parte de confianza, por medio de la implicación de un dispositivo de confianza (TD).

La técnica anterior mencionada anteriormente presenta el inconveniente de implicar un dispositivo de confianza y, más particularmente, componentes especialmente diseñados a los que se asignan Valores de Configuración de Componentes (CCV) específicos almacenados en registros específicos denominados Registros de Configuración de Componentes (CCR). Este mecanismo requiere la modificación de un conjunto entero de componentes que se componen para implementar el proceso y no proporciona ninguna solución para componentes ya existentes.

Claramente, todavía existe una necesidad de una solución global para mejorar la seguridad en los ordenadores y de manera más general, en los sistemas IHS, basada en una amplia variedad de máquinas y sus diversas configuraciones.

Compendio de la invención

Es un objeto de la presente invención mejorar la seguridad en el acceso de un Sistema de Manejo de Información (I.H.S.) según la invención definida en las reivindicaciones adjuntas.

Descripción de los dibujos

Ahora se describirá una realización de la invención, a modo de ejemplo solamente, con referencia a los dibujos anexos, en donde:

La Figura 1 ilustra una estructura básica de un sistema de manejo de información que puede aprovecharse del proceso según la presente invención.

La Figura 2 y la Figura 4 ilustran respectivamente el proceso de calificación y de validación de una primera realización de la invención, que opera en una configuración cliente-servidor.

La Figura 3 y la Figura 5 ilustran respectivamente una segunda realización de la invención donde los procesos de calificación y de validación solamente se ejecutan localmente dentro del sistema 100.

Descripción de la realización preferida de la invención

El proceso y aparato se describirán más particularmente en referencia con la figura 1 que ilustra una estructura básica de un sistema para encarnar la presente invención.

Hablando en términos generales, el sistema puede ser cualquier Sistema de Manejo de Información o dispositivo que esté equipado con recursos de procesamiento. Esto incluye claramente, sin ninguna limitación, ordenadores de sobremesa, ordenadores portables y portátiles, PC de mano o de bolsillo también conocidos como Asistente Personal Digital (P.D.A.) e incluso los últimos teléfonos móviles equipados con recursos de procesamiento.

La Figura 1 ilustra más particularmente la estructura y los componentes de tal sistema 100 que, en la realización preferida, es un ordenador de sobremesa o uno portátil o cualquier ordenador de mano/PDA equipado con componentes de hardware 110 y elementos de software. Los componentes de hardware incluyen una placa base 111 equipada con un procesador, memoria, equipamiento de alimentación y de baterías, y un conjunto de adaptadores o controladores así como buses y puertos de entrada/salida. La placa base coopera con adaptadores especializados, tales como tarjetas de Red de Área Local (L.A.N.) o de Red de Área Extensa (W.A.N), o cualquier tarjeta o adaptador especializado (video o audio) que proporcione funciones especializadas y capacidades de procesamiento.

Además de la placa base, el sistema 100 incluye además un conjunto de dispositivos externos, tales como los dispositivos principales tradicionales 112, es decir, el equipamiento bien conocido de pantalla-teclado-ratón y algunas facilidades de almacenamiento (discos duros, disquetes, unidades CDROM o DVD ROM, etc.). El sistema puede incluir además dispositivos secundarios 113 unidos a la placa base a través de puertos de I/O adecuados, es decir, una impresora, un escáner, equipamiento de vídeo y foto, dispositivos de comunicación (Bluetooth, WIFI, infrarrojos, telefonía GSM-GPRS, módem), y dispositivos incluso más especializados, tales como un lector de identificación por radiofrecuencia (RFID), un lector biométrico y, de manera más general, cualquier otro equipamiento que es probable que sea una fuente de información.

El sistema 100 se opera bajo el control del código de software, que está organizado en un código de bajo nivel 121 - el código conocido de Sistema Básico de Entrada Salida (BIOS) que coopera con el Sistema Operativo (O.S.) y el código de nivel superior que incluye componentes y aplicaciones de software especiales. En la realización preferida de la invención, el sistema 100 se opera bajo el sistema operativo WINDOWS (TM) bien conocido comercializado por MICROSOFT Corp. Un ordenador de mano se puede equipar con el sistema operativo WINDOWS CE (Marca registrada de Microsoft Corp.) diseñado para PC de bolsillo. Claramente, los expertos adaptarán la invención a cualquier sistema operativo alternativo, tal como LINUX o PalmOS (TM), por ejemplo.

Considerando ahora más particularmente la información a la que el sistema 100 puede acceder a través de sus dispositivos de propósito general y más especializados, se puede ver que se da acceso al sistema 100, a través de la interfaz 130, a una amplia gama de información, tal como información contextual o de entorno 131 así como información relacionada con el usuario 132. La información de entorno 131 puede ser, sin ninguna limitación, información con respecto al Sistema de Posicionamiento Global (G.P.S), la fecha y la hora, la temperatura pertinente de la sala en donde está siendo operado el sistema, el número de línea de teléfono proporcionado por el adaptador de módem, la dirección de Control de Acceso al Medio (MAC)/IP asignada por el adaptador de red ... La información relacionada con el usuario 132 puede incluir datos tales como datos biométricos, código PIN, inicio de sesión-contraseña, tarjeta de ID o cualquier información personal proporcionada por el usuario...

Como se ilustra en la figura 1, el sistema 100 se ve como un conjunto de componentes de hardware y de software que se combinan entre sí con el fin de dotar al usuario con un acceso a algunos recursos o la terminación de una transacción dada (por ejemplo con un servidor remoto -no conocido-).

La invención logra una alta seguridad en la transacción o en cualquier servicio realizando sistemáticamente, anterior a cualquier transacción, un procedimiento de autenticación completo que incluye tanto un procedimiento de calificación como uno de validación.

Tanto durante el proceso de calificación como de validación, se identifican, comprueban y validan todos los componentes que forman parte del equipamiento de hardware o de software del sistema que se autentica, como se describirá con detalle en lo sucesivo.

Cada componente dentro del sistema 100 está siendo identificado, registrado y validado a la transacción o anterior a acceder a cualquier servicio seguro. En el marco de la invención del asunto, un *componente* -se entiende que abarca un elemento de hardware y de software que son constituyentes del sistema. Con más precisión, un componente es un elemento constitutivo de un sistema. Puede ser una tarjeta integrada (placa base, tarjeta de adaptador de red), un chip microprocesador, un chip de memoria, un disco duro... De manera más general, un dispositivo periférico (lector biométrico) y un componente de software o programa de aplicaciones se considera que es un componente.

En la realización preferida de la invención, cada componente está asociado a datos de *componentes* que incluyen, sin limitación, Datos de Identificación de Componentes (CID) y Datos Contextuales de Componentes (CCD).

Los Datos de Identificación de Componentes (CID) son un identificador que identifica de forma única el componente en sí mismo. Claramente, puede ser cualquier cadena alfanumérica única que identifique el componente correspondiente, ya sea hardware o software.

Se debería señalar que, en el campo técnico de los ordenadores, es una práctica común de los fabricantes de productos y de los proveedores de piezas individuales asignar referencias que identifican individualmente un elemento en particular. Por ejemplo, cada procesador tiene un número de serie único; cada software instalado (bajo Windows (TM) por ejemplo) (o componente de software como Active X) tiene un Identificador Globalmente Único (GUID) y/o Identificador de Clase (CLSID). Para el software GUID/CLSID, podría no haber ninguna colisión entre dos identificadores en la medida que se construyen para ser únicos en un OS. Para los componentes de hardware, se podría crear un ID de Ordenador concatenando el identificador del fabricante, el identificador del modelo y el número de serie del componente en sí mismo. Claramente, los expertos adaptarán la invención a cualquier sistema operativo alternativo, tal como LINUX.

Tales identificadores se usan particularmente para permitir que los diferentes controladores correspondientes a los diferentes dispositivos sean instalados dentro de un sistema operativo dado, por ejemplo el sistema operativo de tipo Windows (TM).

La invención se aprovecha de los identificadores ya existentes para mejorar la seguridad y la autenticación en las transacciones y el acceso a sistemas de manejo de información.

Además de los Datos de Identificación de Componentes, los datos de Componentes incluyen además unos Datos Contextuales de Componentes (CCD) que no identifican el componente en sí mismo sino que son los datos devueltos por el componente cuando está en uso. Por ejemplo, los CCD son las coordenadas GPS en una solicitud específica proporcionada por un componente de dispositivo GPS. Los datos CID y CDD se pueden combinar para crear una referencia de identificación contextual compleja que se usará para autorizar o denegar el acceso al sistema 100.

Esta identificación compleja se usa en un proceso de autenticación seguro que implica dos procesos sucesivos de calificación y validación que aumentan sustancialmente la seguridad de acceso a la transacción o al servicio. El primer proceso de calificación permite la generación de una Firma de Calificación de Referencia (RQS), que es una instantánea de la configuración autorizada del sistema -que cubre tanto los identificadores de componentes como posiblemente los datos contextuales proporcionados por algunos componentes- cuya firma se usa en un proceso de validación posterior con el propósito de autorizar o denegar el acceso a una transacción o a un servicio.

Se puede ver que la invención se puede usar para una amplia variedad de sistemas y para una amplia variedad de aplicaciones, incluyendo aplicaciones financieras, legales o económicas que implican acceso a datos sensibles. En particular, se puede usar en dos contextos diferentes, asegurando una transacción remota entre el sistema 100 y un servidor distante o incluso, localmente, asegurando el uso del sistema 100.

I. Proceso de calificación

La Figura 2 ilustra una primera realización de un proceso de calificación en una configuración cliente-servidor, donde el sistema 100 se usa para acceder a una transacción o a un servicio desde un servidor remoto (no mostrado en la figura).

El Proceso de calificación se inicia con un paso 201 que consiste en la instalación de un denominado Agente de calificación que se instala dentro del sistema 100. La configuración del Agente de calificación se puede lograr de diferentes formas convencionales: desde unos medios como un CD-ROM o un disquete, a través de una transferencia de descarga (a través de una conexión segura a Internet https por ejemplo). Cuando el sistema 100 se opera bajo un sistema operativo de tipo Windows NT o Windows 2000, se debería señalar que se requieren derechos de administrador para lograr la instalación del Agente de Calificación. Para las aplicaciones más críticas, será útil reservar la ejecución del Proceso de calificación descrito a continuación solamente a personal especializado

que tenga derechos de administrador sobre el ordenador o sistema 100.

El Proceso de calificación entonces procede con un paso 202 donde se crea un denominado Archivo de Calificación del Sistema (SQF) que, en la realización preferida, toma la forma de un archivo de Lenguaje de Marcado Extendido (XML) que se almacena idealmente en un área segura y temporal del sistema (por ejemplo en la memoria o en el disco duro).

El archivo SQF presenta una organización estructurada que permite el almacenamiento de los datos correspondientes a los diferentes componentes detectados dentro del sistema 100, que incluye los Datos de Identificación de Componentes (CID) y, posiblemente, los Datos Contextuales de Componentes (CCD) que se pueden devolver por uno o más componentes particulares. Las partes enteras de información se combinarán en un mismo archivo que se cifrará con el propósito de generar una firma de calificación de referencia que proporcione seguridad mejorada al sistema.

El Archivo de Calificación del Sistema (SQF) se dispone como una plantilla para un archivo de Lenguaje de Marcado Extendido (XML) que está estructurado para proporcionar espacio disponible para recibir, para cada tipo genérico de componente, los CID y los CCD del componente real detectado e identificado dentro del sistema. Preferiblemente, el archivo SQF comprende, en su creación, el denominado Parámetro de Presencia de Componentes (CPP) que son parámetros predefinidos asociados con el tipo genérico de componentes (tales como disco duro, placa base, etc...) que se usarán para asegurar más particularmente tanto el Proceso de Calificación como el de Validación y, de esta manera, aumentar ventajosamente la eficiencia del proceso de autenticación. Los parámetros CPP pueden ser los siguientes:

Obligatorio: el componente correspondiente debe estar presente dentro del sistema para permitir la ejecución completa del proceso de Calificación o del de Validación

Opcional: el componente puede estar presente o no. Su presencia no influye en la ejecución del proceso de Calificación ni del de Validación

Prohibido: el componente no puede estar presente. La detección de la presencia de los componentes detendrá la ejecución del proceso de Calificación o del de Validación.

Más preferiblemente, el archivo SQF se crea seleccionando un archivo particular entre un conjunto de plantillas predefinidas que corresponden a diferentes conjuntos de perfiles o diferentes niveles de seguridad o *calificación*, o incluso a diferentes aplicaciones que se pueden asegurar por el proceso de autenticación. Eso permite organizar diferentes niveles de calificaciones con diferentes configuraciones de componentes que se detectarán, rastrearán y comprobarán por medio de sus parámetros CPP correspondientes.

Preferiblemente, una clasificación de cuatro niveles se organiza por medio de cuatro plantillas distintivas para el archivo SQF, como sigue:

Nivel de calificación 1: confidencial

Nivel de calificación 2: restringido

Nivel de calificación 3: crítico

Nivel de calificación 4: Muy crítico

y/o cada aplicación segura puede requerir su propia plantilla.

Por el bien de la claridad, ahora se detallarán tres ejemplos de archivos SQF correspondientes a tres conjuntos diferentes de calificaciones.

El primer ejemplo que se indica a continuación corresponde a un perfil en donde la placa base, la CPU y la RAM no se pueden cambiar una vez que se completa el proceso de calificación (TOFILL sustituido con CID en el paso 207 de Rellenar datos de Identificador de Componentes).

```
<?xml version="1.0"?>
<Computer QualificationLevel="3">
 <motherboard CPP="mandatory">
  <CID>
   <manufacturer> TOFILL </manufacturer>
   <model> TOFILL </model>
   <chipset> TOFILL </chipset>
  </CID>
 </motherboard>
 <CPU CPP="mandatory">
  <CID>
   <manufacturer> TOFILL </manufacturer>
   <model> TOFILL </model>
   <speed> TOFILL </speed>
   <SN> TOFILL </SN>
  <CID>
 </CPU>
 <RAM CPP="mandatory">
 ...
 </RAM>
```

En ese ejemplo, la placa base, la CPU y la RAM se definen que son “obligatorias” y el campo TOFILL se sustituirá por los datos individuales extraídos durante la detección de los componentes.

El segundo ejemplo muestra una situación donde no se permite que ninguna tarjeta inteligente sea conectada al sistema 100 dado que el parámetro CPP está ajustado a ‘prohibido’, lo que prohíbe la presencia de tal componente durante los procesos de calificación o de validación.

```
<?xml version="1.0"?>
<Computer QualificationLevel="2">
...
...
  <SmartCardReader CPP="prohibited">
  </SmartCardReader>
</Computer>
```

En el tercer ejemplo a continuación, se muestra un perfil que es más preciso sobre modificaciones posteriores y ofrece un nuevo nivel de seguridad dado que almacena en una sección de datos los datos proporcionados por el componente GPS. Se puede ver que las coordenadas geográficas x, y proporcionadas por un componente GPS se recuperan de ese componente y se almacenan dentro del Archivo de Calificación del Sistema. Para aumentar el nivel de seguridad, se asigna al componente GPS un parámetro CPP “obligatorio” y el archivo SQF contiene una sección <CCD> con atributos que definen algunos rangos geográficos predefinidos y ya contenidos en el archivo.

```
<?xml version="1.0"?>
<Computer QualificationLevel="1">
...
  <GPS CPP="mandatory">
   <CID>
    <manufacturer> TOFILL </manufacturer>
    <model> TOFILL </model>
    <SN> TOFILL </SN>
   <CCD>
    <Lattitude RangeMin="-10" RangeMax="+30"> TOFILL </Lattitude>
    <Longitude RangeMin="-50" RangeMax="+50"> TOFILL </Longitude>
   </CCD>
  </GPS>
```

Claramente, los tres ejemplos que se tratan anteriormente se deberían considerar solamente con propósitos de ilustración, sin ninguna limitación, con el fin de demostrar la gran versatilidad y las amplias posibilidades ofrecidas por el proceso de la invención.

Con referencia de nuevo a la figura 2, uno ve que cuando el archivo SQF se crea a partir de una plantilla predefinida tratada anteriormente, el proceso procede con un paso 203 que es un punto de entrada para un bucle, basado en los pasos 203-208, que se usa para detectar, rastrear y registrar los diferentes componentes que se pueden detectar dentro del sistema 100 según la estructura del archivo SQF que se creó en el paso 202.

Para cada componente que se considera dentro del sistema 203, el proceso se refiere al QSF y extrae del mismo - en su caso- el Parámetro de Presencia de Componentes (CPP) correspondiente del QSF. Ese valor se lee en un paso 204.

Entonces, en un paso 205, el proceso comprueba la conformidad del sistema con el parámetro CPP correspondiente al componente que se considera. Esto se logra mediante la detección de la lista de componentes existentes en el sistema y comparando dicha lista con los contenidos de la estructura XML del archivo SQF.

Los expertos pueden usar diferentes métodos y procesos disponibles para determinar los componentes particulares que están presentes dentro del sistema 100. En una realización, el proceso de calificación extrae información del sistema directamente de las tablas SMBIOS, o interroga a la Interfaz de Gestión Distribuida (DMI), o a la Instrumentación de Gestión de Windows (WMI) como se conoce en Microsoft. Como es conocido por los expertos, la interfaz DMI es una Interfaz de Programación de Aplicaciones (API) que consiste en un conjunto de rutinas que se llaman para acceder a la información almacenada dentro de la capa BIOS. La información básica relativa a la interfaz de programación DMI se puede encontrar en la dirección http://www.dmtf.org/spec/html.

Usando la interfaz DMI o WMI o accediendo directamente al nivel SMBIOS, el Proceso de calificación accede a las diferentes tablas contenidas en el BIOS de Gestión del Sistema. (SMBIOS) con el propósito de notificar información exhaustiva con respecto a la configuración de software preferida por el usuario, y requerida para completar una solicitud de transacción. Tal información incluye el tipo de procesador, el tipo de conjunto de chips, el número de unidades de disco duro, la tarjeta gráfica particular que se usa, el número de serie de la pantalla, la referencia del sistema operativo y así sucesivamente.

A continuación se ilustra la determinación, a partir de la API conocida de Windows (TM), de la identificación del disco duro del sistema 100:

```
BOOL GetVolumeInformation(
  LPCTSTR lpRootPathName,
  LPTSTR lpVolumeNameBuffer,
  DWORD nVolumeNameSize,
  LPDWORD lpVolumeSerialNumber,
  LPDWORD lpMaximumComponentLength,
  LPDWORD lpFileSystemFlags,
  LPTSTR lpFileSystemNameBuffer,
  DWORD nFileSystemNameSize
);
```

De manera similar, el proceso puede acceder al nivel de BIOS para determinar los diferentes componentes, tal como sigue:

```
class Win32_BIOS : CIM_BIOSElement
{
 uint16 BiosCharacteristics[];
 string BIOSVersion[];
 string BuildNumber;
 string Caption;
 string CodeSet;
 string CurrentLanguage;
 string Description;
 string IdentificationCode;
 uint16 InstallableLanguages;
 datetime InstallDate;
 string LanguageEdition;
 String ListOfLanguages[];
 string Manufacturer;
 string Name;
 string OtherTargetOS;
 boolean PrimaryBIOS;
 datetime ReleaseDate;
 string SerialNumber;
 string SMBIOSBIOSVersion;
 uint16 SMBIOSMajorVersion;
 uint16 SMBIOSMinorVersion;
 boolean SMBIOSPresent;
 string SoftwareElementID;
 uint16 SoftwareElementState;
 string Status;
 uint16 TargetOperatingSystem;
 string Version;
};
```

Estos son solamente ejemplos que muestran lo fácil que es reunir información valiosa con respecto a los diferentes componentes que forman un sistema, y derivar la información de CID y CCD que se ha de ser introducida dentro del archivo SQF.

Con referencia de nuevo a la figura 2, uno ve que si no se satisface la conformidad en el paso 205, entonces el proceso procede a un paso 206 que interrumpe el proceso de calificación. Claramente, esto significa que el sistema 100 se considerará como que es un sistema NO CALIFICADO que se puede usar para tareas normales o de rutina pero ciertamente no para acceder a información o transacciones sensibles o críticas. Esto es una gran ventaja del proceso de la invención que permite que sean llevadas modificaciones a un ordenador (por ejemplo, enchufando algunos dispositivos externos) y continuar usando el sistema para tareas “normales” y de rutina. Por el contrario, cuando el sistema se aplica para calificación, el sistema tendrá que estar en una condición predefinida -incluyendo la configuración de hardware y de software- para permitir la terminación del proceso de calificación y la creación de la firma de referencia que se tratará más adelante.

Si se satisface la conformidad, entonces el proceso procede a un paso 207 donde la información asociada con el componente correspondiente, es decir, los Datos de Identificación de Componentes (CID) y los Datos Contextuales de Componentes (CCD) recuperados de dicho componente, está siendo introducida con precisión en la ubicación adecuada (campo FILLIN) dentro de la estructura XML del archivo SQF. Si un componente es un captador biométrico, entonces los CID identificarán el captador mientras que el CCD puede consistir, por ejemplo, en una imagen de mapa de bits en bruto de una huella digital del usuario. Por consiguiente, integra datos de usuario en la información reunida dentro de la plantilla de archivo de protocolo de calificación. Del mismo modo, en caso de que un componente sea un receptor GPS, el proceso de calificación lee los identificadores de hardware del receptor (CID) y los datos GPS proporcionados por dicho receptor (CCD) y tal información se almacena dentro de la estructura XML del archivo SQF.

El proceso entonces procede con un paso 208 donde se considerará el siguiente componente en la plantilla del archivo SQF y el proceso volverá al punto de entrada 203.

Cuando todos los componentes han sido procesados, el proceso procede con un paso 209 donde el Archivo de Calificación del Sistema (SQF) está siendo cifrado por un algoritmo de cifrado (tal como RSA, PGP… basado en claves públicas y privadas). El mecanismo de cifrado particular que se usa no es parte de la presente invención y no se desarrollará además. Claramente, los expertos adaptarán la invención a cualquier algoritmo de cifrado conocido.

El resultado del proceso de cifrado permite derivar una denominada Firma de Calificación de Referencia (RQS) que permite que la configuración entera del sistema -incluyendo componentes de hardware y de software (CID) e incluso datos contextuales (CDD) sea almacenada dentro de la misma firma.

Se describió que los datos CID y CCD se introdujeron dentro de la plantilla del archivo SQF con el fin de derivar un archivo SQF completo único. Alternativamente, el archivo SQF de origen puede permanecer como una plantilla y los datos CID y los de CDD se pueden almacenar en un archivo separado, lo que da como resultado la generación de dos archivos cifrados: un primer archivo que contiene el CPP que define el nivel de calificación y un segundo archivo que contiene los datos CID y CDD recuperados de todos los componentes. Pero, preferiblemente, el Proceso de calificación genera una Firma de Calificación de Referencia (RQS) Única -basada en un archivo SQF cifrado único- que abarca los datos CPP, CID y CID.

En un paso 210, el proceso entonces realiza una transferencia segura de la firma RQS al sistema remoto y esta última se almacena entonces en un paso 211. Preferiblemente, la firma de calificación de referencia RQS se envía a través de protocolos remotos seguros comunes (tales como HTTP, VPN ...). El servidor remoto entonces almacena la firma de calificación en relación con el sistema (en una base de datos o un archivo XML) con el fin de ser capaz de acceder a esta información durante un Proceso de validación posterior.

El Proceso de calificación entonces realiza en un paso 212 la eliminación del Agente de calificación del sistema 100 y se completa el Proceso de calificación.

La Figura 3 ilustra una realización alternativa donde el Proceso de calificación se usa para aumentar la seguridad de uso de un sistema, considerado per se, es decir, con independencia de cualquier conexión a cualquier servidor.

Los pasos 201 a 209 son respectivamente los mismos que los pasos 301 a 309. Después del cifrado del archivo SQF, el proceso almacena entonces este último en un área protegida del sistema en un paso 310. Entonces, en un paso 311, el proceso procede con la supresión del agente de calificación del sistema.

Por lo tanto, las dos realizaciones que se ilustran respectivamente en la figura 2 y la Figura 3 difieren entre sí por el hecho de que, en un caso, la Firma de Calificación de Referencia RQS se almacena dentro del sistema mientras que, en el otro caso, se carga en el servidor remoto lo que aumenta ciertamente el nivel de la seguridad.

Se puede observar que el Proceso de calificación que se describió anteriormente aumenta sustancialmente el nivel de la seguridad dado que todos los componentes que constituyen el sistema 100 son cuidadosamente detectados, comprobados y sus CID y CCD internos recuperados según el Archivo de Calificación del Sistema SQF predefinido. En particular, cualquier sistema que no cumpla totalmente con los requisitos enumerados en el archivo SQF -y particularmente con los Parámetros de Presencia de Componentes (CPP) definidos dentro del mismo- no estará calificado para proporcionar una transacción o acceso seguro al sistema.

Esta ventaja significativa resulta de la combinación, para el proceso de calificación que se describió anteriormente, de un proceso de validación que toma en consideración la firma de referencia que se generó previamente.

II. Proceso de validación posterior

Además, la autenticación del sistema 100 se mejora sustancialmente mediante el uso del proceso de validación que se describirá ahora y que, de nuevo, ejecutará una comprobación completa de un sistema que solicita la validación, anterior a permitir que tal sistema complete cualquier transacción o acceda a datos críticos.

La Figura 4 ilustra el proceso de validación de la invención en una configuración de cliente servidor.

El proceso de validación comienza con un paso 401 donde, de manera similar al paso 201 de la figura 2, un agente de validación está siendo instalado dentro del sistema que solicita una transacción con el servidor o cualquier tipo de servicio remoto.

El proceso entonces procede con un paso 402 donde el agente de validación crea un Archivo de Calificación del Sistema SQF correspondiente al nivel de calificación que se requiere del sistema 100. Preferiblemente, el proceso genera una plantilla que tiene la misma estructura que la plantilla usada en el paso 202 de la figura 2 y que tiene de esta manera el Parámetro de Presencia de Componentes (CPP) correspondiente.

El proceso entonces procede con un paso 403 que es un punto de entrada de un bucle 403-408 usado para procesar por separado todos los componentes que se ajustan a la lista identificada dentro del archivo SQF.

En un paso 404, el proceso de validación extrae el parámetro CPP de la plantilla y, en un paso 405, realiza una operación de detección (usando métodos similares a los tratados anteriormente) para comprobar la conformidad del sistema real con el CPP que se enumera.

Si la comprobación de conformidad falla, entonces la validación se interrumpe en un paso 406 y entonces se deniega al usuario el acceso a la transacción o al recurso, en un paso 414.

Por el contrario, si la comprobación de conformidad tiene éxito en el paso 405, entonces el proceso procede con un paso 407 en donde los datos CID y CCD se recuperan del componente correspondiente y se usan para rellenar los archivos SQF.

El paso 408 se usa para considerar el siguiente componente dentro de la lista de componentes genéricos definidos en el archivo SQF y el proceso vuelve al paso 403 para procesar este nuevo componente.

Cuando todos los componentes fueron procesados, el proceso entonces procede con un paso 409 que cifra el archivo SQF totalmente completado con el fin de generar una Firma de Comprobación (CS) desde allí.

Entonces, el proceso procede con un paso 410 donde la firma de comprobación (CS) se transmite al servidor remoto.

El paso 411 es un paso opcional donde el agente de validación se puede eliminar del sistema que solicita la validación.

Entonces, el proceso procede con un paso 412 donde se realiza una prueba en el servidor con el fin de determinar si la firma de comprobación CS es igual a la Firma de Calificación de Referencia que se calculó durante el Proceso de Calificación del sistema y se almacenó dentro del servidor remoto.

En una realización preferida, el servidor remoto genera un ID de sesión temporal (o una marca de tiempo) en el paso 401 que también se comprobará en el paso 412. Si el ID de sesión ha expirado (por ejemplo, puede ser por una razón de tiempo de espera entre los pasos 401 y 412), se denegará el acceso. Este procedimiento adicional mejora la seguridad.

Si la prueba tiene éxito, entonces esto significa que el sistema que solicita la validación cumple totalmente con todos los requisitos contenidos con el archivo SQF cifrado (y de esta manera protegido). En particular, esto asegura que todos los CID y los CCD (incluyendo las coordenadas biométricas o de GPS cuando sean aplicables) son totalmente compatibles.

El acceso a la transacción o al servicio se autoriza de esta manera en un paso 413 y el proceso de validación se completa entonces en un paso 415 que puede ser el final de la conexión.

Por el contrario, si la prueba del paso 412 falla, eso significa que el sistema 100 no es totalmente compatible con los requisitos enumerados dentro de la RQS almacenada dentro del servidor, por ejemplo, debido a que algunas partes internas del sistema fueron cambiadas o que el usuario no es el usuario registrado y, de esta manera, el acceso a la transacción o al servicio se deniega en un paso 414. El proceso entonces procede con el paso 415 que es el final del proceso de validación.

La figura 5 muestra una realización alternativa del proceso de validación que se usa en una configuración local con el propósito de asegurar un acceso al sistema 100 supuesto que está en una configuración autónoma.

El proceso de validación implica los pasos 501-509 que son idénticos a los pasos 401-409 del proceso de validación en la configuración remota. De hecho, se instala un agente de validación (paso 501) con el propósito de crear un archivo SQF en el sistema (paso 502) y, para cada componente que tiene un tipo enumerado dentro del archivo SQF, se leen los parámetros CPP (paso 504), luego se comprueba su conformidad (paso 505). Los datos CID y los CDD contextuales se recuperan entonces con el propósito de rellenar el archivo SQF.

Cuando se genera la Firma de Comprobación (CS) en un paso 509, entonces el proceso va directamente a un paso 512 en donde se lee la Firma de Calificación del Sistema de Referencia desde el almacenamiento local y se compara con la firma de comprobación en un paso 512.

Si la comparación tiene éxito, entonces el proceso va a un paso 513 donde se permite el acceso a la transacción o al servicio.

Por el contrario, si la prueba del paso 509 falla, entonces el proceso de validación procede con un paso 514 donde se deniega al sistema 100 el acceso a la transacción o al servicio.

El proceso de validación se completa entonces en un paso 515.

Se ha descrito cómo llega a ser posible aumentar de manera eficiente la seguridad de acceso a un sistema generando la denominada firma de calificación del sistema de referencia que abarca todos los componentes de hardware y de software, así como los Datos de Componentes Contextuales, en la medida que se usa tal firma en el proceso de validación. Esta es una desviación muy ventajosa de las firmas tradicionales unidas a los componentes individuales del sistema operativo Windows conocido donde la firma se usa para detectar el daño del componente correspondiente, con el propósito de sustituir cualquier componente dañado por una nueva versión.

En la invención, la Firma de calificación del sistema de referencia no se proporciona por el fabricante del producto del componente, sino que se genera automáticamente por el nuevo proceso de calificación que se describió anteriormente, con el propósito de proporcionar una referencia que se puede usar dentro del proceso de validación y asegurar de esta manera el acceso al sistema IHS o a la transacción.

III. Aplicación de la invención

Se debería señalar que la invención que se describió anteriormente se puede usar en una gama de aplicaciones.

La invención se puede aplicar directamente al uso de la tarjeta de ID nacional. De hecho, algunos países, incluyendo Francia, están reconsiderando la generalización de un nuevo tipo de tarjetas de ID que integran un chip electrónico para contener datos biométricos digitales del portador. En Francia, con el fin de permitir a los ayuntamientos recopilar los datos biométricos de los ciudadanos que piden una tarjeta de ID, el gobierno proporciona equipos móviles, que se transportan de un ayuntamiento a otro, para registrar la información. No hace falta decir lo esencial que es que esos equipos móviles no sean manipulados, con el fin de asegurarse de que solamente se usan por personal de la administración autorizado, y que la información biométrica registrada no se modifica o extrae indebidamente después de su registro. Solamente se debería permitir entonces a los sistemas y usuarios aprobados registrar y transmitir información al servidor central que controla la producción de los documentos de ID, se debería comprobar la integridad de toda la cadena y el proceso debería ser completamente trazable.

De manera más general, la información biométrica generalizada en pasaportes está en curso. Para proteger la privacidad de los ciudadanos que viajan, es importante asegurarse de que sus datos biométricos no se recogen indebidamente cuando se identifican a sí mismos. Por lo tanto, solamente se deberían usar sistemas calificados y totalmente validados para procesar tal información, y debería ser comprobable la integridad de los sistemas.

Además, los departamentos judiciales y de policía en Europa tendrán pronto acceso al registro penal europeo de todos los ciudadanos. También accederán a las bases de datos de Schengen (SIS). Es importante:

1. asegurar que solamente el personal autorizado accede a estas bases de datos

2. permitir la trazabilidad de los accesos

3. hacer cumplir incluso las regulaciones más estrictas para controlar quién modifica el contenido de las bases de datos.

La identidad del personal se controlará, por lo tanto, a través de un mecanismo más seguro que sólo un inicio de sesión/contraseña. Es probable que sea adoptado el uso de tarjetas de ID biométrico. El acceso a los datos se realizará tanto a través de terminales fijos como móviles. En todos los casos, es necesario permitir al servidor verificar que el sistema no ha sido manipulado, permitiendo por ejemplo evitar la comprobación biométrica o desviar los datos consultados. El hardware y en cierta medida el software del terminal de consulta debe ser comprobable por el servidor antes de conceder acceso a los datos.

La invención también se puede usar para proporcionar un servicio de garantía eficiente por un fabricante de productos. En caso de alquiler de un ordenador, por ejemplo, puede ser de interés para la empresa que proporciona el sistema estar segura de que el sistema es idéntico cuando vuelve del arrendamiento con respecto a la configuración que tenía cuando se envió al cliente.

Cuando se vende un ordenador (o cualquier servidor electrónico), la invención proporciona una forma rápida y fácil de comprobar si el ordenador ha sido abierto y modificado por el cliente. Definitivamente sustituye la vieja e insegura etiqueta adhesiva de garantía.

Durante el tiempo de alquiler, la innovación proporciona una solución técnica para asegurar cambios no autorizados mediante comprobaciones remotas. Esto es particularmente valioso para algunas aplicaciones cuando se desea que no ocurra ninguna modificación no autorizada en un ordenador o un sistema, a partir de un ajuste preconfigurado, predefinido y registrado. Se hacen posibles con la invención nuevas posibilidades de arrendamiento o de alquiler comercial.

Otra ventaja del uso de la invención es la posibilidad de controlar el acceso al servicio desde la ubicación física de dicha máquina.

REIVINDICACIONES

1. Un proceso para asegurar el acceso a los recursos de un Sistema de Manejo de Información (I.H.S.), dicho I.H.S. que comprende un conjunto de componentes de hardware que incluyen información representativa del fabricante, modelo y número de serie de dichos componentes de hardware, comprendiendo dicho I.H.S. además un Sistema Operativo (O.S.) usado para ejecutar aplicaciones y proporcionar una Interfaz de Programación Aplicaciones (API) para acceder a dicha información representativa del fabricante, modelo y número de serie de dichos componentes de hardware, dicho proceso que implica los pasos de iniciar un proceso de calificación preliminar basado en la detección de los componentes de dicho sistema, seguido por la generación de una firma de calificación de referencia;

- un proceso de validación posterior a dicho proceso de calificación que comprende, anterior a cualquier transacción con o acceso a un servidor remoto, una detección adicional de los componentes con el propósito de generar una nueva firma a ser comparada con dicha firma de calificación de referencia,

caracterizado por que

dicho proceso de calificación implica los pasos de:

- detectar un conjunto de componentes presentes dentro de dicho sistema usando dicha Interfaz de Programación de Aplicaciones para acceder a dicha información representativa del fabricante, modelo y número de serie de dichos componentes de hardware, y

- generar para cada componente de hardware unos Datos de Identificación de Componentes (CID) concatenando dicha información representativa del fabricante, modelo y dicho número de serie, para completar un archivo de calificación del sistema (SQF) que enumere dichos componentes con los correspondientes Datos de Identificación de Componentes (CID);

- cifrar dicho archivo de calificación del sistema con el fin de crear una firma de calificación de referencia (RQS);

- transmitir y almacenar dicha firma de calificación de referencia (RQS) en dicho servidor remoto;

- dicho proceso de validación implica

- realizar una nueva identificación y detección de los componentes de hardware y una generación posterior de un nuevo archivo de calificación del sistema;

- cifrar dicho nuevo archivo de calificación del sistema con el fin de generar una firma de comprobación;

- comparar dicha firma de comprobación con dicha firma de calificación de referencia (RQS) almacenada dentro de dicho servidor remoto y, en respuesta a dicha comparación, permitir o denegar el acceso a dicha transacción con o dicho acceso a dicho servidor remoto.

2. Un proceso según la reivindicación 1 caracterizado por que dicho archivo de calificación del sistema está organizado bajo una forma estructurada, que enumera un conjunto de componentes genéricos asociado con parámetros de presencia de componentes (CPP) definiendo si la presencia del componente es obligatoria, está prohibida o es opcional.

3. Un proceso según la reivindicación 2, caracterizado por que dicho proceso de calificación o dicho proceso de validación comprueba la conformidad de cada componente identificado con dicho sistema con el parámetro de presencia de componentes (CPP) correspondiente.

4. Un proceso según la reivindicación 2, caracterizado por que dicho proceso de calificación genera un archivo de calificación del sistema que se elige entre un conjunto de plantillas predefinidas correspondientes a diferentes niveles de seguridad o diferentes aplicaciones.

5. Un proceso según la reivindicación 2, caracterizado por que dicho archivo de calificación del sistema comprende, para cada componente genérico que se enumera, un conjunto de campos que recibe Datos de Identificación de Componentes (CID) que identifican dicho componente y Datos Contextuales de Componentes (CCD) para almacenar datos recuperados por dicho componente.

6. Un proceso según cualquiera de las reivindicaciones precedentes, caracterizado por que se usa durante una sesión de comunicación entre dicho sistema y un servidor remoto y que la Firma de calificación de referencia se almacena dentro de dicho servidor y se elimina de dicho sistema con el fin de asegurar un acceso a dicho servidor.

7. Un proceso según la reivindicación 6, caracterizado por que una solicitud de sesión de validación está limitada en tiempo por un periodo predeterminado y el servidor hace que el proceso de validación falle después de la expiración de dicho periodo.

8. Un proceso según cualquiera de las reivindicaciones precedentes, caracterizado por que un componente es un receptor GPS que proporciona los CID que identifican dicho receptor y que proporciona rangos de coordenadas (x,y) que se usan y almacenan en dicho archivo de calificación del sistema como datos contextuales de componentes (CCD).

9. Un proceso según cualquiera de las reivindicaciones precedentes, caracterizado por que un componente es un sensor biométrico que proporciona datos de CID que identifican dicho sensor y datos biométricos que se usan como CDD en dicho archivo de calificación del sistema.

10. Un proceso según cualquiera de las reivindicaciones precedentes, caracterizado por que un componente es un lector de tarjetas inteligentes que proporciona datos de CID que identifican dichos sensor y datos de tarjetas inteligentes que se usan como CCD en dicho archivo de calificación del sistema.

11. Un programa informático de seguridad para asegurar el acceso a los recursos de un Sistema de Manejo de Información (I.H.S.), dicho producto de programa informático de componentes que tiene elementos de código de programa para llevar a cabo un método según cualquiera de las reivindicaciones 1 a 10.

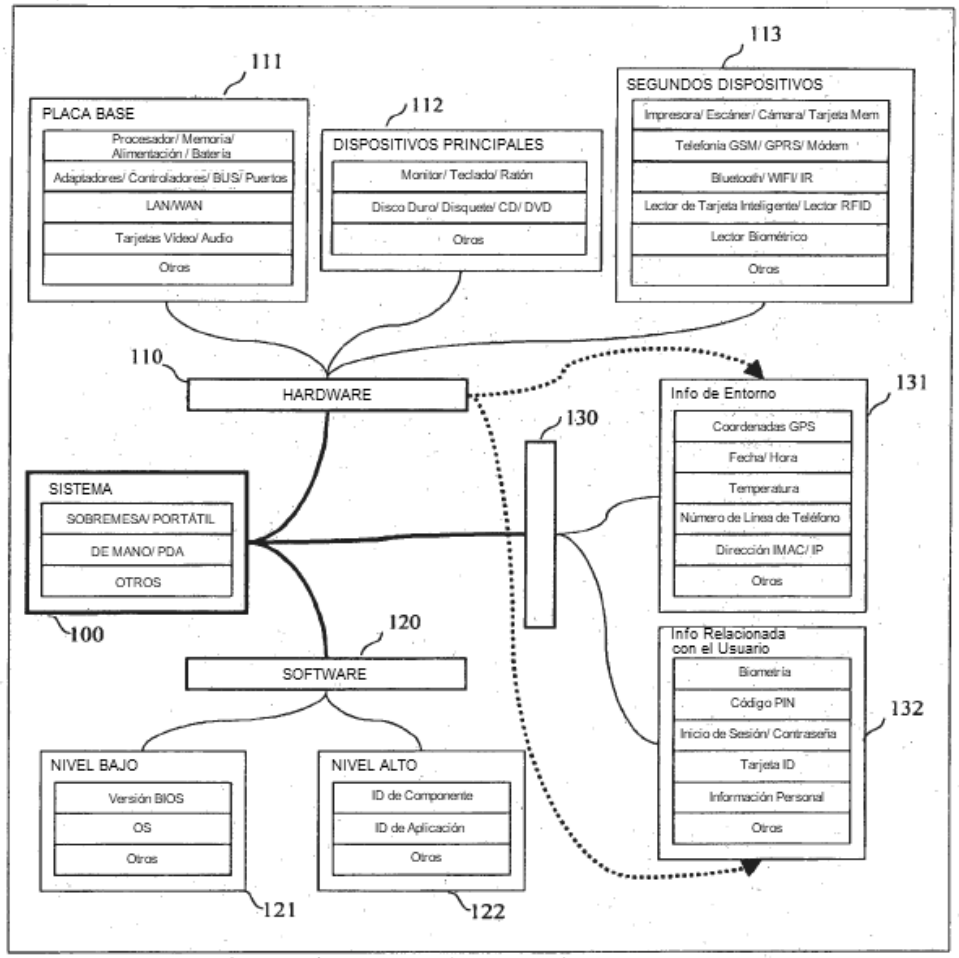
111
PLACA BASE
Procesador/ Memoria/ Alimentación / Batería
Adaptadores/ Controladores/ BUS/ Puertos
LAN/WAN
Tarjetas Video/ Audio
Otras
112
DISPOSITIVOS PRINCIPALES
Monitor/ Teclado/ Ratón
Disco Duro/ Disquete/ CD/ DVD
Otras
113
SEGUNDOS DISPOSITIVOS
Impresora/ Escáner/ Cámara/ Tarjeta Mem
Telefonía GSM/ GPRS/ Módem
Bluetooth/ WIFI/ IR
Lector de Tarjeta Inteligente/ Lector RFID
Lector Biométrico
Otras
110
HARDWARE
130
131
Info de Entorno
Coordenadas GPS
Fecha/ Hora
Temperatura
Número de Línea de Teléfono
Dirección IMAC/ IP
Otras
SISTEMA
SOBREMESA/ PORTÁTIL
DE MANO/ PDA
OTROS
100
120
SOFTWARE
Info Relacionada con el Usuario
Biometría
Código PIN
Inicio de Sesión/ Contraseña
Tarjeta ID
Información Personal
Otras
132
NIVEL BAJO
Versión BIOS
OS
Otras
121
NIVEL ALTO
ID de Componente
ID de Aplicación
Otras
122

Fig. 1

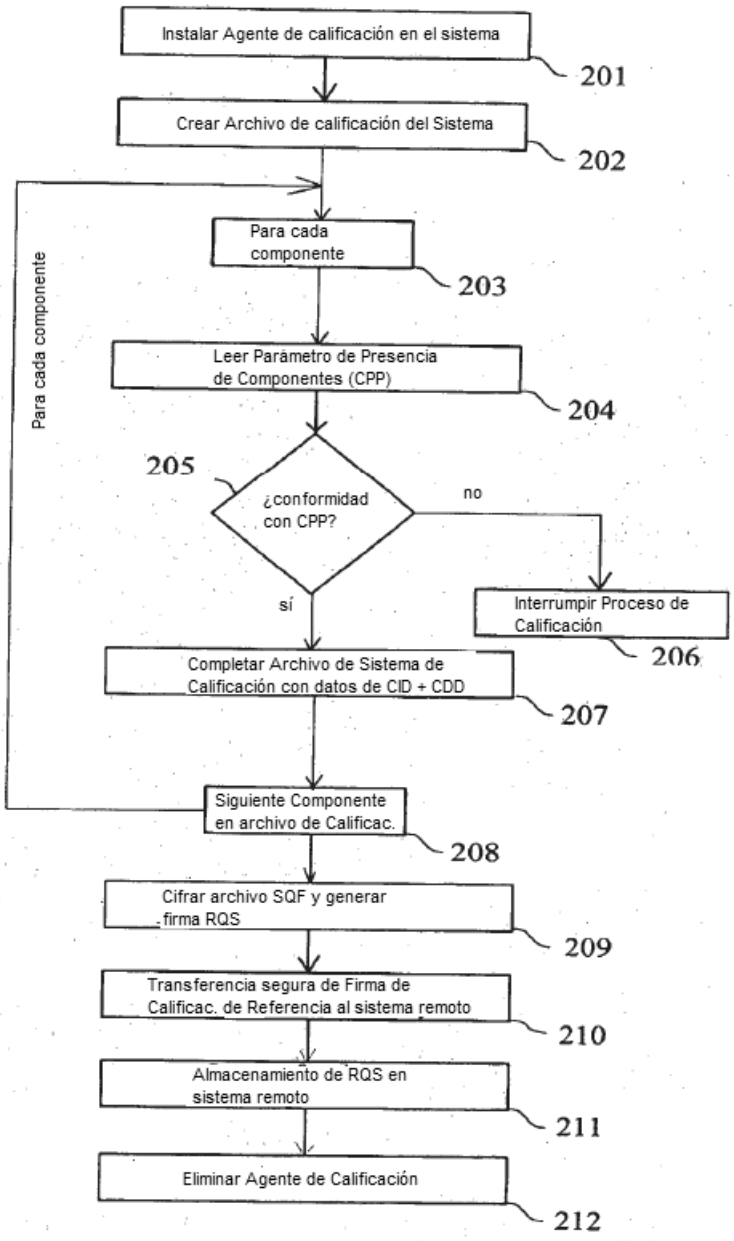

Fig. 2: Proceso de Calificación (Remoto)

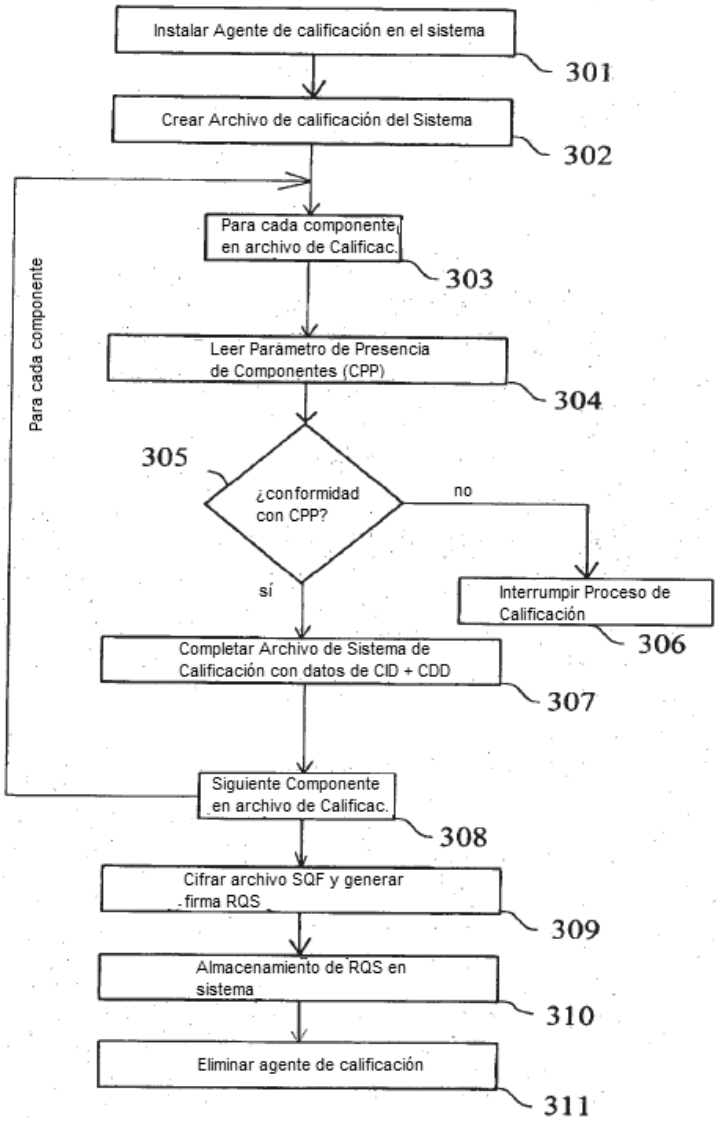

Fig. 3: Proceso de Calificación (local)

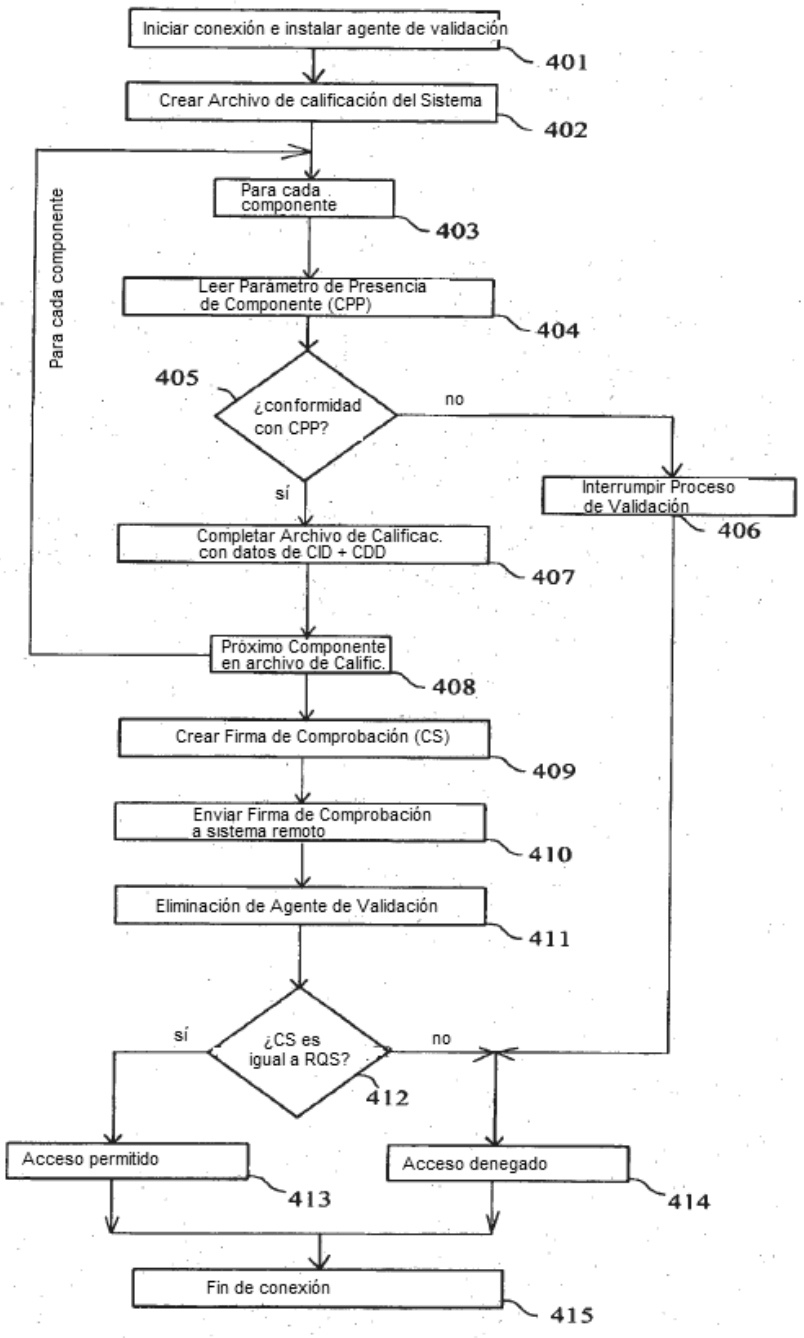

Fig. 4: Proceso de Validación (remoto)

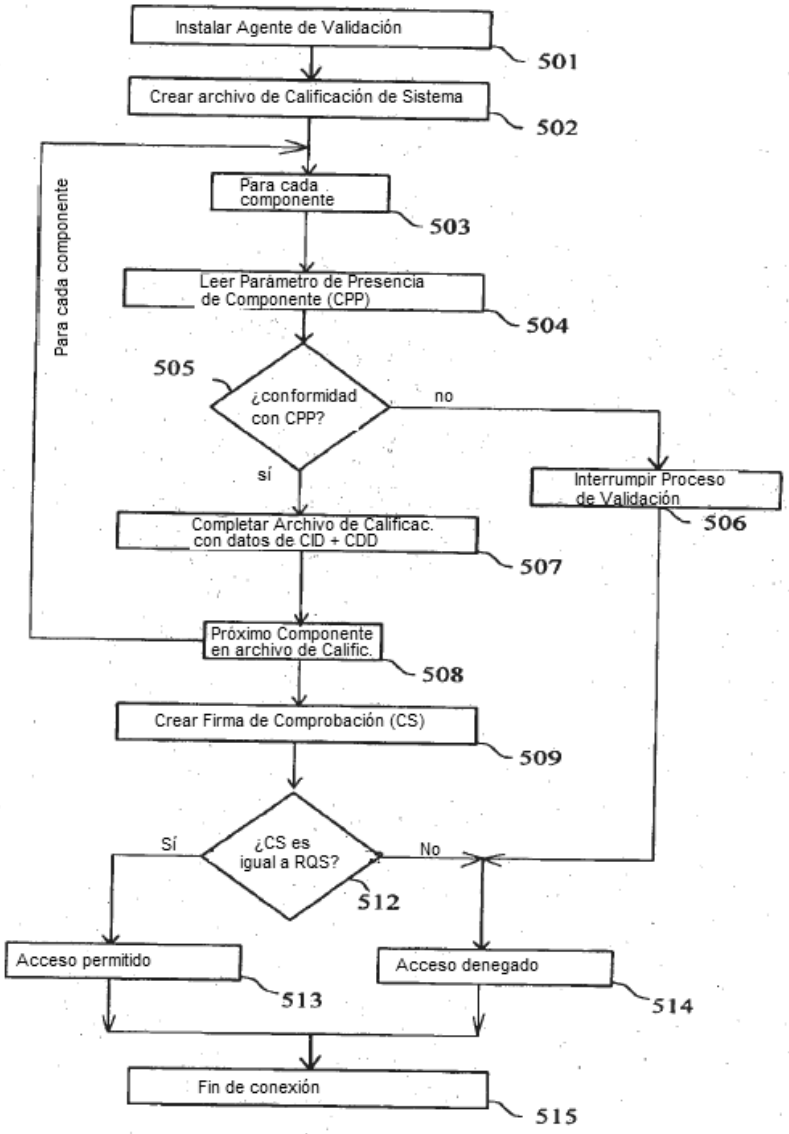

Fig. 5: Proceso de Validación (local)