(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 690 828**

(51) Int. CI.:

G06F 21/44 (2013.01)
H04L 29/06 (2006.01)
G06F 21/33 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.12.2013 PCT/US2013/078397**

(87) Fecha y número de publicación internacional: **10.07.2014 WO14107443**

(96) Fecha de presentación y número de la solicitud europea: **31.12.2013 E 13822076 (9)**

(97) Fecha y número de publicación de la concesión europea: **18.07.2018 EP 2941730**

(54) Título: **Protección de recursos en dispositivos no fiables**

(30) Prioridad:

02.01.2013 US 201313732526

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.11.2018

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052, US

(72) Inventor/es:

MENDELOVICH, MEIR y
MATCHORO, RON

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Protección de recursos en dispositivos no fiables

Antecedentes

Los ordenadores y los sistemas informáticos han afectado casi todos los aspectos de la vida moderna. Los ordenadores generalmente están involucradas en el trabajo, diversión, cuidado de la salud, transporte, entretenimiento, administración del hogar, etc.

Además, la funcionalidad del sistema informático se puede mejorar mediante la capacidad de un sistema informático para interconectarse con otros sistemas informáticos a través de conexiones de red. Las conexiones de red pueden incluir, pero sin limitación, conexiones a través de Ethernet por cable o inalámbricas, conexiones celulares o incluso conexiones de ordenador a ordenador a través de conexiones en serie, en paralelo, USB u otras. Las conexiones permiten a un sistema informático acceder a servicios en otros sistemas informáticos y recibir de forma rápida y eficiente datos de aplicaciones de otros sistemas informáticos.

Las redes actuales han permitido que se conecten en red muchos tipos nuevos y diferentes de dispositivos. Además, existe un deseo de tener movilidad con dispositivos en red. La movilidad continúa evolucionando, a medida que los teléfonos inteligentes y las tabletas son más frecuentes en las redes de empresas comerciales. Muchas organizaciones que desean aprovechar la oportunidad de aumentar la productividad de los empleados adoptan el estilo de trabajo móvil y permiten que los trabajadores de la información accedan a los recursos empresariales desde sus dispositivos móviles.

Si bien esta tendencia brinda nuevas oportunidades para mejorar la efectividad de los empleados, también crea nuevos riesgos de seguridad para los administradores de la IT ya que en muchos casos un empleado puede almacenar credenciales empresariales (por ejemplo, un par de nombre de usuario y contraseña) en sus dispositivos móviles. Por ejemplo, la mayoría de los clientes de correo electrónico móvil que usan Active Sync disponible de Microsoft Corporation of Redmond Washington requieren credenciales de la empresa. Estas credenciales se pueden extraer fácilmente del dispositivo móvil. Por ejemplo, el dispositivo puede ser robado, el dispositivo puede albergar una aplicación móvil que resulta ser un caballo de Troya que recopila contraseñas guardadas o registra las pulsaciones de teclas. Esto puede ser particularmente peligroso puesto que a menudo un usuario de una empresa puede usar las mismas credenciales para acceder a la mayoría, si no a todos, los recursos disponibles para el usuario de la empresa.

La materia objeto reivindicada en la presente memoria descriptiva no está limitada a realizaciones que resuelven cualquier desventaja o que operan solo en entornos tales como los que se han descrito más arriba. Por el contrario, este antecedente solo se proporciona para ilustrar un área de tecnología ejemplar en la que se pueden poner en práctica algunas realizaciones que se describen en la presente memoria descriptiva.

El documento US 2003/005299 A1 se refiere a un sistema de gestión de autorización de usuario que utiliza una meta - contraseña y el procedimiento para la misma. Un procedimiento de gestión de la información de autenticación de usuario recibe una meta - contraseña de un usuario. Un repositorio enumera las direcciones de red y los identificadores asociados, teniendo cada identificador una contraseña codificada asociada. Se intercepta una respuesta de autenticación del usuario. Se genera una respuesta de autenticación modificada identificando una dirección de red a la que se dirige la respuesta, buscando la dirección de red identificada en el repositorio, se identifica un tratamiento correspondiente a la dirección en función de la búsqueda, se decodifica la contraseña asociada con el tratamiento utilizando la meta - contraseña como una clave de decodificación, y se sustituye la contraseña decodificada por la meta - contraseña en la respuesta de autenticación. El procedimiento también genera contraseñas pseudoaleatorias consistentes con reglas de contraseña. El repositorio puede residir en un dispositivo cliente, un servidor proxy, una red de área local o un servidor de seguridad que tenga una dirección de protocolo de Internet (IP). El repositorio también puede estar dispuesto en un servicio de base de datos.

Sumario

El objeto de la presente invención es proporcionar un procedimiento y sistema para autenticar a un usuario a un primer servicio para permitir que el usuario acceda a un recurso proporcionado por el primer servicio.

Este objeto se resuelve por la materia objeto de las reivindicaciones independientes.

Las realizaciones preferidas están definidas en las reivindicaciones dependientes.

Una realización ilustrada en la presente memoria descriptiva incluye un procedimiento que puede practicarse en un entorno informático. El procedimiento incluye actos para autenticar a un usuario a un primer servicio para permitir que el usuario acceda a un recurso proporcionado por el primer servicio. El recurso es un recurso protegido que requiere una credencial de propósito general (por ejemplo, un nombre de usuario y / o contraseña) para acceder al

recurso. El procedimiento incluye recibir en un segundo servicio, desde el dispositivo, una credencial ad - hoc. La credencial ad - hoc es una credencial que es particular para el dispositivo. La credencial ad - hoc puede ser usada para autenticar tanto al usuario como al dispositivo, pero no puede ser usada directamente como autenticación en el primer servicio para que el usuario acceda al recurso. El procedimiento incluye además, en el segundo servicio, sustituir la credencial de propósito general por la credencial ad - hoc y reenviar la credencial de propósito general al primer servicio. De esta manera, el primer servicio puede proporcionar el recurso al usuario en el dispositivo.

Este Sumario se proporciona para presentar una selección de conceptos en una forma simplificada que se describe con más detalle a continuación en la Descripción detallada. Este Sumario no pretende identificar las características clave o las características esenciales de la materia reivindicada, ni está destinado a ser utilizado como una ayuda para determinar el alcance de la materia objeto reivindicada.

Las características y ventajas adicionales se expondrán en la descripción que sigue, y en parte serán obvias a partir de la descripción, o pueden ser aprendidas mediante la práctica de las enseñanzas de la presente memoria descriptiva. Las características y ventajas de la invención pueden ser realizadas y obtenerse por medio de los instrumentos y combinaciones indicados particularmente en las reivindicaciones adjuntas. Las características de la presente invención se harán más evidentes a partir de la descripción que sigue y de las reivindicaciones adjuntas, o pueden ser aprendidas mediante la práctica de la invención como se expone a continuación.

Breve descripción de los dibujos

Con el fin de describir la manera en la que se pueden obtener las ventajas y características que se han mencionado más arriba y otras, una descripción más particular del tema que se ha descrito brevemente más arriba se representará mediante referencia a realizaciones específicas que se ilustran en los dibujos adjuntos. Se debe entender que estos dibujos representan solo realizaciones típicas y, por lo tanto, no deben considerarse de alcance limitativo, las realizaciones se describirán y se explicarán con especificidad y detalles adicionales mediante el uso de los dibujos adjuntos en los que:

La figura 1 ilustra un sistema para gestionar las credenciales primaria y secundaria del usuario; y

La figura 2 ilustra un procedimiento para autenticar a un usuario en un primer servicio para permitir que el usuario acceda a un recurso proporcionado por el primer servicio.

Descripción detallada

Las realizaciones pueden incluir la funcionalidad para proteger credenciales primarias de propósito general al emitir credenciales secundarias dedicadas que se usarán solo en contextos específicos, como interfaces empresariales específicas, protocolos específicos, buzones de correo específicos, etc. (por ejemplo, una credencial solo puede ser usada desde la interfaz ActiveSync disponible de Microsoft® Corporation of Redmond Washington) y / o dispositivos y que pueden tener un ciclo de vida esperado por separado. Si estas credenciales secundarias se ven comprometidas, el daño será limitado. En particular, el daño puede estar limitado solo al dispositivo al que se aplican las credenciales secundarias, solo a aquellas ciertas interfaces empresariales a las que se aplican las credenciales secundarias, y / o al período de tiempo limitado durante el que las credenciales secundarias son válidas. Por lo tanto, los daños pueden ser limitados en comparación con el caso en el que se comprometen las credenciales empresariales primarias, que permiten el acceso a un sistema empresarial completo o a partes grandes de un sistema empresarial.

Por lo tanto, y con referencia a la figura 1, algunas realizaciones implementan una credencial secundaria 102 (tal como una contraseña) para dispositivos no fiables, tales como el dispositivo 104. Por ejemplo, el dispositivo 104 puede ser un dispositivo móvil.

Las realizaciones implementan una pasarela 106 que reemplaza la credencial secundaria 106 con la credencial primaria 108 (por ejemplo, la credencial primaria de toda la empresa). La coexistencia de una credencial primaria 108 y una credencial secundaria 102 puede implementarse sin cambiar los sistemas internos del dispositivo 104 o varios servicios o sistemas en una red empresarial 110 implementando una pasarela 106. La pasarela 106 puede estar separada del cliente 104. La pasarela 106 puede ser capaz de representar por proxy el tráfico relevante para las aplicaciones 112 en la red de la empresa 110 y cambiará la credencial secundaria 102 con la credencial primaria 108 para permitir el acceso a los recursos de la empresa.

En muchos casos, esta pasarela 106 reside en el borde de la red empresarial 110. La pasarela 106 se implementa de forma que todo el tráfico exterior debe pasar por la pasarela 106 para entrar en la red empresarial 110. De esta manera, el acceso a una aplicación 112 desde dentro de la red de la empresa 110 requerirá el uso de la credencial primaria 108. Por ejemplo, la figura 1 ilustra que un usuario puede usar un sistema corporativo en la instalación 114, tal como un ordenador de sobremesa o un ordenador portátil, ubicado en las instalaciones de una empresa y conectado a la red de la empresa 110 por hardware y líneas de comunicación bajo el control directo del administrador de la red de la empresa 110. En este caso, como se ilustra, la credencial primaria 108 se puede enviar desde el sistema corporativo 114 a un servicio 116 para acceder a los recursos 118 de una aplicación 112.

Alternativamente, cuando un usuario desea acceder a los recursos 118 proporcionados por la aplicación 112 cuando está conectado de forma remota, la credencial secundaria especial 102 puede ser utilizada por el sistema cliente 104 que envía la credencial secundaria 102 a la pasarela 106 en la que se usa para sustituir la credencial primaria 108 para permitir que el recurso 118 sea devuelto al sistema cliente 104. Se debe hacer notar que las realizaciones pueden implementarse cuando no todo el tráfico se envía a la pasarela 106. Más bien, en algunas realizaciones, solo ciertos tipos de tráfico o tráfico destinado a ciertas aplicaciones pueden ser enviados a la pasarela 106. Por ejemplo, los datos de correo electrónico y calendario pueden enviarse a la pasarela 106, mientras que otro tráfico no se enruta a través de la pasarela 106.

La credencial secundaria 102 puede estar sujeta a políticas diferentes que la credencial primaria 108. Por ejemplo, la credencial secundaria 102 puede estar limitada más temporalmente que la credencial primaria. Por ejemplo, la credencial secundaria puede ser válida durante un período de tiempo más corto que la credencial primaria 108. Alternativa o adicionalmente, la credencial secundaria 102 puede tener límites temporales más restrictivos que la credencial primaria 108 con respecto a cuándo puede ser usada. Por ejemplo, la credencial primaria 108 puede ser usada a cualquier hora del día o de la noche, mientras que la credencial secundaria 102 se puede limitar a, por ejemplo, entre las 5:00 p.m. y las 9:00 a.m. Estas políticas podrían ser aplicadas por la pasarela 106.

La pasarela 106 puede imponer restricciones de nivel de servicio o aplicación con respecto a la credencial secundaria 102. Por ejemplo, aunque la credencial primaria 108 puede ser usada para acceder virtualmente a cualquier recurso disponible para un usuario dado al que pertenece la credencial primaria 108, la pasarela 106 puede restringir al mismo usuario que accede a los recursos de la empresa a través del dispositivo 104 y usar la credencial secundaria 102 en un conjunto limitado de aplicaciones o recursos. Por ejemplo, la pasarela puede sustituir a la credencial primaria 108 cuando se hacen solicitudes para recursos de correo electrónico, pero puede negarse a sustituir la credencial primaria por solicitudes que se realizan desde el cliente 104 para recursos de bases de datos confidenciales. Algunas de tales realizaciones pueden estar basadas en roles. Por ejemplo, la pasarela 106 puede exigir menos restricciones (o ninguna) al CEO o al administrador primario de la red de la empresa, mientras que se imponen más restricciones a un administrativo de entrada de datos.

La pasarela 106 puede realizar el intercambio de credenciales de la credencial secundaria 102 por la credencial primaria 108 en base a una base de datos 120 que correlaciona la credencial primaria 108 y la credencial secundaria 102 que son gestionadas por un sistema de gestión 122.

Este sistema de gestión 122 puede asignar credenciales secundarias en base a la entrada proporcionada a una interfaz de usuario o / y a su lógica interna. El sistema de gestión 122 también puede definir políticas de uso y caducidad. Este sistema de gestión típicamente implementará una lógica de autenticación adicional para generar y proporcionar autenticación secundaria a usuarios y dispositivos, tales como los dispositivos 104. En un ejemplo ilustrativo, un usuario accede al sistema de gestión 122 usando la Web UI. El usuario se autentica mediante una tarjeta inteligente u otra autenticación. A continuación, el usuario recibe, a través de la web UI, credenciales secundarias en forma de una contraseña ad - hoc que es válida por una semana para ActiveSync. Por lo tanto, el usuario puede obtener una credencial secundaria 102 que puede ser usada con un dispositivo no fiable 104, en el que la credencial secundaria está limitada en el tiempo en cuanto a cuánto tiempo es válida y está limitada a ciertas aplicaciones.

Además, en algunas realizaciones, la credencial secundaria 102 puede ser generada de una manera que solo permita que se use con ciertos dispositivos (por ejemplo, el dispositivo 104) o ciertos canales. Por ejemplo, la pasarela 106 puede hacer cumplir restricciones que permiten que la credencial secundaria 102 se use con un dispositivo específico 104 o conjunto de dispositivos, al mismo tiempo que excluye su uso con otros dispositivos. La pasarela 106 puede ser capaz alternativa o adicionalmente de limitar la credencial secundaria 102 para usar con ciertos canales de comunicación. Por ejemplo, la credencial secundaria puede ser usada con una red doméstica particular de un usuario, pero no puede ser usada cuando el dispositivo está conectado a ciertas redes públicas Wi - Fi o redes celulares.

Las credenciales secundarias, tal como la credencial 102, pueden ser generadas de diferentes maneras. Por ejemplo, en algunas realizaciones, la credencial secundaria 102 puede ser generada usando un secreto en el sistema de gestión 122 y las credenciales primarias 108. Se puede realizar un hash u otro cálculo sobre el uso del secreto en el sistema de gestión y las credenciales primarias para generar la credencial secundaria 102.

En otra realización, la credencial secundaria 102 puede ser seleccionada o generada manualmente por un usuario después de que el usuario presente la credencial primaria 108 a través de una web UI del sistema de gestión 122.

La explicación que sigue a continuación se refiere a un número de procedimientos y actos de procedimientos que pueden ser realizados. Aunque los actos de procedimiento pueden discutirse en un orden determinado o ilustrarse en un diagrama de flujo que se realiza en un orden particular, no se requiere un orden particular a menos que se indique específicamente o se requiera porque un acto depende de que otro acto se complete antes de que el acto sea realizado.

Con referencia a continuación a la figura 2, se ilustra un procedimiento 200. El procedimiento 200 puede practicarse en un entorno informático. El procedimiento 200 incluye actos para autenticar a un usuario a un primer servicio para permitir que el usuario acceda a un recurso proporcionado por el primer servicio. El recurso es un recurso protegido que requiere una credencial de propósito general (por ejemplo, un nombre de usuario y / o contraseña) para acceder al recurso. Por ejemplo, como se ilustra en la figura 1, un usuario puede tener acceso al recurso 108 desde el servicio 116 presentando la credencial primaria 108.

El procedimiento incluye recibir en un segundo servicio desde el dispositivo una credencial ad - hoc (acto 202). La credencial ad - hoc es una credencial que es particular del dispositivo, y puede ser usada para autenticar tanto al usuario como al dispositivo, pero no puede ser usada directamente como autenticación en el primer servicio para que el usuario acceda al recurso. Por ejemplo, el dispositivo 104 puede recibir del sistema de gestión 122 la credencial secundaria 102. La credencial secundaria 102 puede ser una credencial que es específica del dispositivo 104 en el sentido de que cuando se usa la credencial con el dispositivo 104 se puede usar como autenticación, pero cuando se usa con otros dispositivos, no se puede usar como autenticación. En algunas realizaciones, la credencial debe ser usada con uno o más canales particulares y no puede ser usada con otros canales. En algunas realizaciones, la credencial puede ser válida solo para un único dispositivo particular, mientras que en otras realizaciones es válida para un conjunto de dispositivos previamente especificado.

El procedimiento 200 incluye además, en el segundo servicio, sustituir la credencial de propósito general por la credencial ad - hoc y reenviar la credencial de propósito general al primer servicio (acto 204). Por ejemplo, como se ilustra en la figura 1, la credencial primaria 108 es sustituida por la credencial secundaria 102. La credencial primaria 108 se usa para obtener el recurso 108 para el usuario en el dispositivo 104. Por lo tanto, la acción 204 se puede realizar de tal manera que el primer servicio (por ejemplo, el servicio 116) puede proporcionar el recurso al usuario en el dispositivo (por ejemplo, el dispositivo 104).

El procedimiento 200 puede practicarse cuando la credencial ad - hoc es una credencial que es particular para un canal de comunicación dado. Por ejemplo, una credencial secundaria puede ser usada para ser usada con una red Wi - Fi pública, mientras que una credencial diferente puede ser usada con una red doméstica, mientras que todavía una credencial diferente puede ser usada con una red celular, etc.

El procedimiento 200 puede practicarse cuando la credencial ad - hoc está temporalmente limitada, de manera que la credencial ad - hoc expira después de un período de tiempo dado. Por lo tanto, por ejemplo, la credencial secundaria 102 puede ser útil solo durante un período de tiempo dado después de ser emitida o después de su primer uso.

El procedimiento 200 puede ser practicado cuando el uso de la credencial ad - hoc en el segundo servicio está limitado por política. Por ejemplo, la política puede limitar el uso de la credencial ad - hoc en tiempo. Por ejemplo, el uso de la credencial puede limitarse a ciertos momentos del día, durante un tiempo limitado consecutivo o total, etc. En algunas realizaciones, la política limita el uso de la credencial ad - hoc al limitar a qué recursos se puede acceder usando la credencial ad - hoc. Por ejemplo, como se ha explicado más arriba, la pasarela 106 puede limitar a qué aplicaciones, servicios o recursos se puede acceder cuando se usa la credencial secundaria 102. Se pueden implementar realizaciones en las que la política limita el uso de la credencial ad - hoc de acuerdo con el rol del usuario. Como se ha explicado previamente, la pasarela 106 puede imponer restricciones por las cuales los usuarios más privilegiados pueden acceder a un conjunto mayor de recursos con credenciales secundarias que los usuarios menos privilegiados.

El procedimiento 200 puede ser practicado cuando la credencial ad - hoc se genera usando la credencial de propósito general y un secreto mantenido por el segundo servicio para calcular la credencial ad - hoc. Como se ha explicado más arriba, el sistema de gestión 122 puede generar las credenciales secundarias 102 realizando un cálculo usando un secreto en el servidor de gestión 122 y las credenciales primarias 108. Alternativamente, el sistema de gestión puede generar aleatoriamente las credenciales secundarias y luego asociarlas con las credenciales primarias. En otra alternativa más, un usuario puede ser capaz de seleccionar o proporcionar su propia credencial secundaria, que a continuación podría ser asociada con la credencial primaria por el sistema de gestión 122.

Además, los procedimientos pueden ser practicados por un sistema informático que incluye uno o más procesadores y medios legibles por ordenador tales como una memoria informática. En particular, la memoria informática puede almacenar instrucciones ejecutables por ordenador que cuando son ejecutadas por uno o más procesadores hacen que se realicen diversas funciones, tales como las acciones enumeradas en las realizaciones.

Las realizaciones de la presente invención pueden comprender o utilizar un ordenador de propósito especial o de propósito general que incluye hardware informático, como se analiza en mayor detalle a continuación. Las realizaciones dentro del alcance de la presente invención también incluyen medios físicos y otros medios legibles por ordenador para transportar o almacenar instrucciones ejecutables por ordenador y / o estructuras de datos. Tales medios legibles por ordenador pueden ser cualquier medio disponible al que se pueda acceder mediante un sistema informático de propósito general o de propósito especial. Los medios legibles por ordenador que almacenan las ins-

trucciones ejecutables por ordenador son medios físicos de almacenamiento. Los medios legibles por ordenador que llevan instrucciones ejecutables por ordenador son medios de transmisión. Por lo tanto, a modo de ejemplo, y no de limitación, las realizaciones de la invención pueden comprender al menos dos tipos claramente distintos de medios legibles por ordenador: medios físicos de almacenamiento legibles por ordenador y medios de transmisión legibles por ordenador.

Los medios físicos de almacenamiento legibles por ordenador incluyen RAM, ROM, EEPROM, CD - ROM u otro disco óptico de almacenamiento (tal como CD, DVD, etc.), almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar medios de código de programa deseados en forma de instrucciones ejecutables por ordenador o estructuras de datos y al que se puede acceder mediante un ordenador de propósito general o de propósito especial.

Una "red" se define como uno o más enlaces de datos que permiten el transporte de datos electrónicos entre sistemas informáticos y / o módulos y / u otros dispositivos electrónicos. Cuando la información se transfiere o se proporciona a través de una red u otra conexión de comunicaciones (ya sea cableada, inalámbrica o una combinación de cableada o inalámbrica) a un ordenador, el ordenador ve adecuadamente la conexión como un medio de transmisión. Los medios de transmisión pueden incluir una red y / o enlaces de datos que pueden ser usados para transportar medios de código de programa deseados en forma de instrucciones ejecutables por ordenador o estructuras de datos y a los que se puede acceder por medio de un ordenador de propósito general o de propósito especial. Las combinaciones de lo anterior también están incluidas dentro del alcance de los medios legibles por ordenador.

Además, cuando se alcanzan diversos componentes del sistema informático, los medios de código de programa en forma de instrucciones ejecutables por ordenador o las estructuras de datos pueden ser transferidos automáticamente desde medios de transmisión legibles por ordenador a medios físicos de almacenamiento legibles por ordenador (o viceversa). Por ejemplo, las instrucciones ejecutables por ordenador o estructuras de datos recibidas a través de una red o enlace de datos pueden almacenarse en memoria RAM dentro de un módulo de interfaz de red (por ejemplo, una "NIC") y a continuación ser transferidos a la RAM del sistema informático y / o a medios de almacenamiento físico legibles por ordenador menos volátiles en un sistema informático. Por lo tanto, los medios físicos de almacenamiento legibles por ordenador se pueden incluir en los componentes del sistema informático que también (o incluso primariamente) utilizan medios de transmisión.

Las instrucciones ejecutables por ordenador comprenden, por ejemplo, instrucciones y datos que hacen que un ordenador de propósito general, un ordenador de propósito especial o un dispositivo de procesamiento de propósito especial realice una cierta función o grupo de funciones. Las instrucciones ejecutables por ordenador pueden ser, por ejemplo, instrucciones binarias de formato intermedio como el lenguaje ensamblador o incluso el código fuente. Aunque el objeto se ha descrito en un lenguaje específico para las características estructurales y / o los actos metodológicos, se debe entender que el objeto definido en las reivindicaciones adjuntas no está necesariamente limitado a las características o actos que se han descrito más arriba. Por el contrario, las características y actos descritos se muestran como formas ejemplares de implementación de las reivindicaciones.

Los expertos en la materia apreciarán que la invención se puede practicar en entornos informáticos de red con muchos tipos de configuraciones de sistemas informáticos, que incluyen ordenadores personales, ordenadores de sobremesa, ordenadores portátiles, procesadores de mensajes, dispositivos manuales, sistemas multiprocesador, productos electrónicos de consumo basados en microprocesador o programables, PC de red, miniordenadores, ordenadores centrales, teléfonos móviles, PDA, buscapersonas, enrutadores, conmutadores y otros similares. La invención también puede ser practicada en entornos de sistemas distribuidos en los que los sistemas informáticos locales y remotos, que están vinculados (ya sea mediante enlaces de datos cableados, enlaces de datos inalámbricos o mediante una combinación de enlaces de datos cableados e inalámbricos) a través de una red, ambos realizan tareas. En un entorno de sistema distribuido, los módulos de programa pueden ubicarse en dispositivos de almacenamiento de memoria tanto locales como remotos.

Alternativamente, o además, la funcionalidad que se ha descrito en la presente memoria descriptiva puede ser realizada, al menos en parte, por uno o más componentes de lógica de hardware. Por ejemplo, y sin limitaciones, los tipos ilustrativos de componentes lógicos de hardware que se pueden utilizar incluyen matrices de puertas programables en el campo (FPGA), circuitos integrados específicos de programas (ASIC), productos estándar específicos de programas (ASSP), sistemas de un sistemas de chip (SOC), dispositivos lógicos programables complejos (CPLD), etc.

La presente invención puede ser realizada en otras formas específicas sin apartarse de sus características. Las realizaciones que se describen deben considerarse en todos los aspectos solo como ilustrativas y no restrictivas. El alcance de la invención, por lo tanto, está indicado por medio de las reivindicaciones adjuntas más que por la descripción anterior. Todos los cambios que se encuentran dentro del significado y el rango de equivalencia de las reivindicaciones deben incluirse dentro de su alcance.

REIVINDICACIONES

1. En un entorno informático, un procedimiento para autenticar a un usuario en un primer servicio (116) dentro de una red empresarial (110) para permitir al usuario acceder a un recurso (118) proporcionado por el primer servicio, en el que el recurso es un recurso protegido que requiere una primera credencial de usuario (108) para acceder al recurso, comprendiendo el procedimiento:

   recibir (202) en una pasarela (106), desde el dispositivo una segunda credencial de usuario (102), en el que la segunda credencial de usuario es una credencial que es particular del dispositivo, y puede ser usada para autenticar tanto al usuario como al dispositivo, pero no puede ser usada directamente como autenticación en el primer servicio para que el usuario acceda al recurso, en el que todo el tráfico externo debe pasar por la pasarela para entrar en la red de la empresa; y

   en la pasarela (106), sustituir (204) la primera credencial de usuario por la segunda credencial de usuario y reenviar la primera credencial de usuario al primer servicio, de manera que el primer servicio pueda proporcionar el recurso al usuario en el dispositivo.

2. El procedimiento de la reivindicación 1, en el que la segunda credencial de usuario es una credencial que es particular para un canal de comunicación dado.

3. El procedimiento de la reivindicación 1, en el que la segunda credencial de usuario está limitada temporalmente, de manera que la segunda credencial de usuario expira después de un período de tiempo dado.

4. El procedimiento de la reivindicación 1, en el que el uso de la segunda credencial de usuario en el segundo servicio está limitado por política.

5. El procedimiento de la reivindicación 4, en el que la política limita el uso de la segunda credencial de usuario por tiempo.

6. El procedimiento de la reivindicación 4, en el que la política limita el uso de la segunda credencial de usuario al limitar a qué recursos se puede acceder usando la segunda credencial de usuario.

7. El procedimiento de la reivindicación 4, en el que la política limita el uso de la segunda credencial de usuario de acuerdo con la función del usuario.

8. El procedimiento de la reivindicación 1, en el que la segunda credencial de usuario se genera utilizando la primera credencial de usuario y un secreto mantenido por el segundo servicio para calcular la segunda credencial de usuario.

9. Un sistema que comprende medios adaptados para realizar el procedimiento de una de las reivindicaciones 1 a 8.

10. Un medio legible por ordenador que almacena en el mismo instrucciones ejecutables por ordenador que, cuando son llevadas a cabo por un procesador, hacen que el procesador realice el procedimiento de cualquiera de las reivindicaciones 1 a 8.

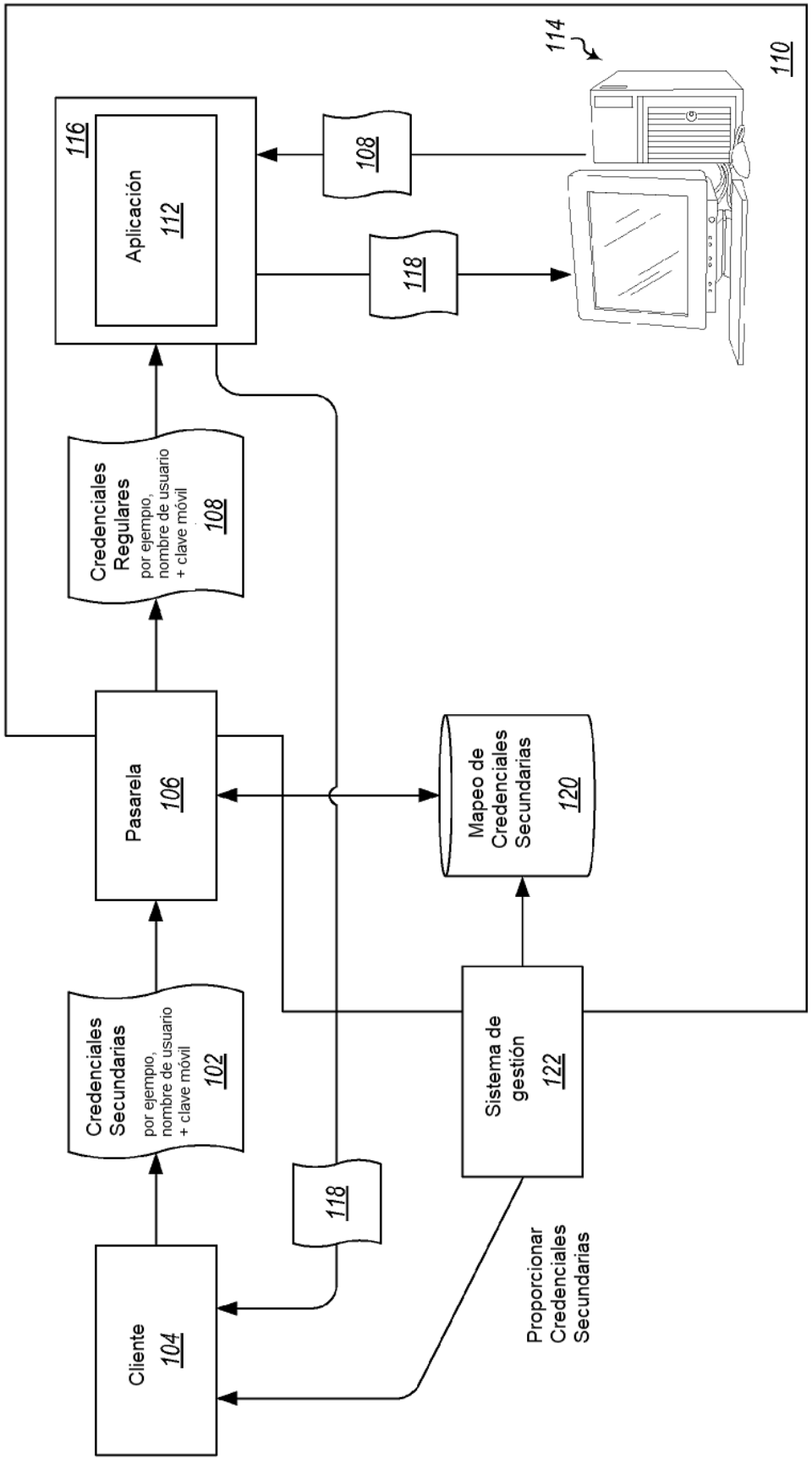
Cliente
104
Credenciales Secundarias
por ejemplo, nombre de usuario + clave móvil
102
Pasarela
106
Credenciales Regulares
por ejemplo, nombre de usuario + clave móvil
108
Aplicación
112
116
118
Mapeo de Credenciales Secundarias
120
Sistema de gestión
122
Proporcionar Credenciales Secundarias
114
110

Figura 1

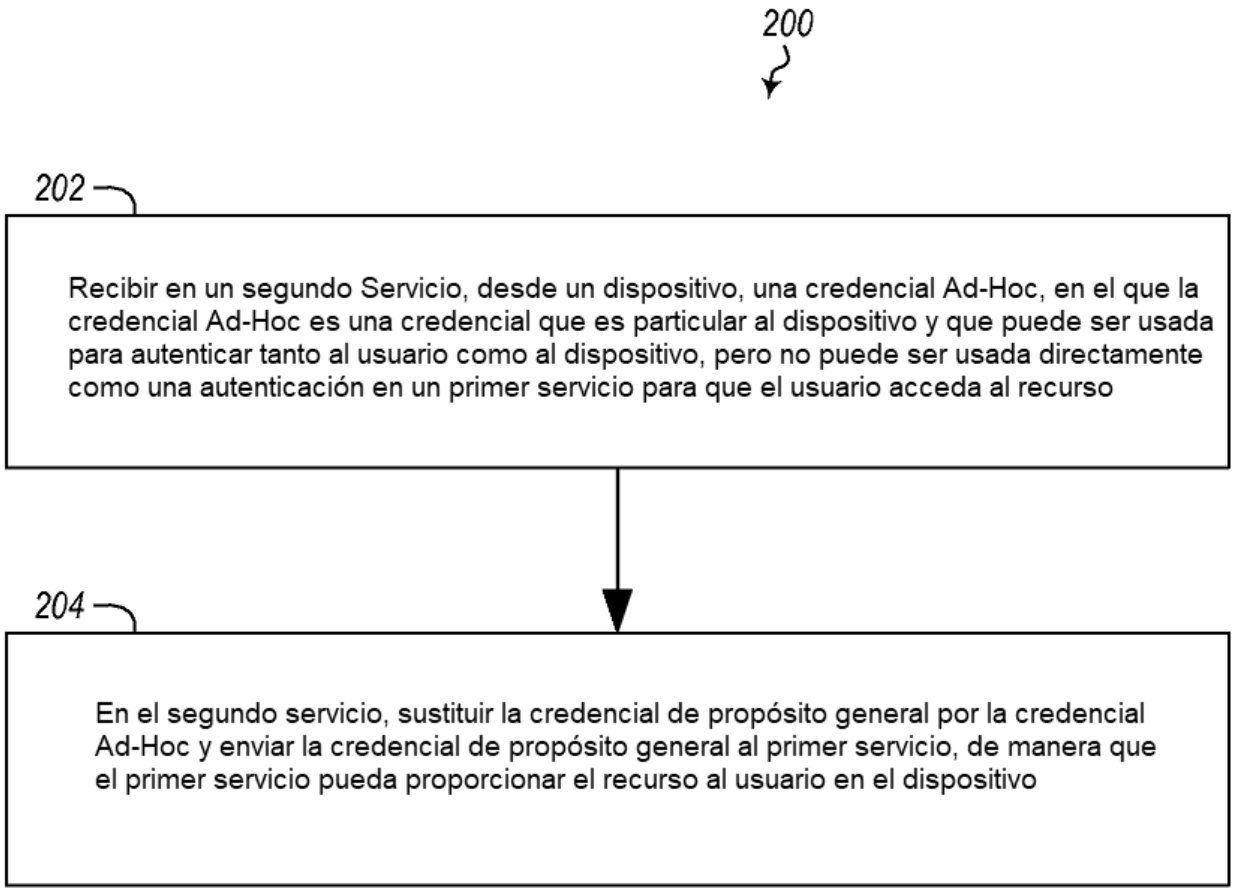
200
202
Recibir en un segundo Servicio, desde un dispositivo, una credencial Ad-Hoc, en el que la credencial Ad-Hoc es una credencial que es particular al dispositivo y que puede ser usada para autenticar tanto al usuario como al dispositivo, pero no puede ser usada directamente como una autenticación en un primer servicio para que el usuario acceda al recurso
204
En el segundo servicio, sustituir la credencial de propósito general por la credencial Ad-Hoc y enviar la credencial de propósito general al primer servicio, de manera que el primer servicio pueda proporcionar el recurso al usuario en el dispositivo

Figura 2