(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 533 757**

(21) Número de solicitud: 201490042

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

13.10.2011

(43) Fecha de publicación de la solicitud:

14.04.2015

(71) Solicitantes:

EVOLIUM MANAGEMENT, S. L. (100.0%)
Passeig de Gràcia, 18, 2º 2ª
08007 Barcelona ES

(72) Inventor/es:

GASPAR CUEVAS, José

(74) Agente/Representante:

ZEA CHECA, Bernabé

(54) Título: **Operaciones criptográficas**

(57) Resumen:

Sistema para realizar una operación criptográfica, que comprende un sistema cliente y un sistema servidor; comprendiendo dicho servidor un gestor de múltiples repositorios, repositorios de claves criptográficas, un procesador y una memoria; y comprendiendo dicho cliente un procesador y una memoria; en el que dichas dos memorias almacenan instrucciones ejecutables por ordenador que, cuando son ejecutadas, hacen que el cliente y el servidor realicen un procedimiento que comprende: enviar, por parte del cliente, una solicitud de la operación criptográfica al servidor; obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas permitidas para la solicitud de los repositorios de claves criptográficas; establecer, por parte del gestor de múltiples repositorios, una clave criptográfica referenciada en dicho conjunto de referencias como la clave criptográfica que se va a utilizar; solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica a utilizar; obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio que ha realizado la operación criptográfica; y enviar, por parte del servidor, el resultado de la operación criptográfica al cliente.

ES 2 533 757 A1

OPERACIONES CRIPTOGRÁFICAS

DESCRIPCIÓN

La presente invención se refiere a un procedimiento de realizar una operación criptográfica, y a un sistema adecuado para llevar a cabo dicho procedimiento.

La invención también se refiere a un procedimiento de obtener un resultado de una operación criptográfica en un sistema informático cliente, y a un producto de programa informático y un sistema informático cliente adecuados para llevar a cabo dicho procedimiento.

La invención se refiere además a un procedimiento de proporcionar un resultado de una operación criptográfica desde un sistema informático servidor, y a un producto de programa informático y un sistema informático servidor adecuados para llevar a cabo dicho procedimiento.

ESTADO DE LA TÉCNICA ANTERIOR

Con el fin de identificar una empresa o un individuo en el mundo digital existen diferentes tipos de claves criptográficas que permiten, por ejemplo, el uso de certificados digitales emitidos y autorizados por autoridades habilitadas tal como *Verisign*, *Thawtee* y muchas otras. Estos certificados digitales permiten que su usuario/propietario relacionado realice operaciones de firma y/o autenticación criptográfica en nombre del propietario/usuario del certificado, de tal manera que dicho propietario/usuario puede representar digitalmente a éste mismo o a su empresa en una amplia gama de diferentes tipos de operaciones electrónicas.

Estas operaciones electrónicas pueden comprender la validación de una identidad simple en transacciones comerciales no críticas, como por ejemplo, para obtener acceso a un sitio web o a una intranet o a cualquier otro sistema corporativo, pero, por otra parte, estas operaciones electrónicas pueden comprender la validación de una identidad crítica en operaciones privilegiadas que pueden comprometer legalmente a toda la empresa. Por lo tanto, parece ser muy importante para una empresa tener bajo control todas o al menos parte de las claves criptográficas que pueden ser utilizadas por los empleados en el mundo digital. En las grandes organizaciones, por ejemplo, puede haber miles de certificados disponibles para los empleados.

Algunas plataformas conocidas permiten realizar operaciones criptográficas con certificados digitales que están instalados localmente en ordenadores de usuario final. Pero, dicha dispersión de claves criptográficas hace que sea difícil de evitar y/o detectar en un período de tiempo razonable usos erróneos y/o maliciosos de algunos de dichos certificados, los cuales, como se ha comentado antes, pueden comprometer a toda la empresa.

Son conocidos sistemas que tratan de evitar dicho control inexistente y/o deficiente de claves criptográficas, estando basados dichos sistemas en el principio de almacenar y gestionar certificados de forma centralizada. Por ejemplo, en las direcciones URL http://www.realsec.com/pdfProEn/CryptoSignServer-technical-information.pdf y http://www.realsec.com/pdfProEn/CryptosignServer.pdf, se describe una plataforma hardware/software de *Realsec* que proporciona un repositorio seguro centralizado de certificados, el cual garantiza la seguridad en los procesos de firma y validación electrónica en servicios orientados a sistemas informáticos. Este repositorio seguro de certificados es un HSM (*Hardware Security Module* – Módulo de Seguridad Hardware) con capacidades de seguridad muy potentes.

Este sistema de *Realsec* permite que una organización almacene remotamente claves criptográficas de una manera centralizada para una mejor supervisión, lo cual supera las desventajas derivadas de tener las claves criptográficas de la empresa almacenadas localmente en ordenadores de usuario final y, por lo tanto, dispersas entre una pluralidad de ordenadores de usuario final. Además, el sistema de *Realsec* ofrece unas funcionalidades muy fuertes de seguridad basadas en el mencionado HSM para todas las claves que permanecen en el sistema.

Sin embargo, el sistema de *Realsec* presenta el inconveniente de no tener un buen equilibrio entre las capacidades proporcionadas de almacenamiento/gestión centralizada y las capacidades proporcionadas de seguridad. Una empresa normalmente tiene diferentes tipos de claves criptográficas con diferentes niveles de criticidad, de manera que el coste de mantener las claves más críticas en el sistema de *Realsec* puede estar justificado, pero el coste de mantener las claves menos críticas en el sistema de *Realsec* puede no ser razonable en absoluto. En otras palabras, el sistema de *Realsec* puede ser funcionalmente adecuado para centralizar el almacenamiento y la gestión de todos los certificados de la empresa, pero, al mismo tiempo, puede proporcionar unas funcionalidades de seguridad excesivamente potentes para algunos de los certificados, tales como los que tienen un nivel de criticidad bajo, en cuyo caso puede ser innecesariamente costoso mantener y gestionar dichos certificados menos críticos en

el sistema de *Realsec*.

EXPLICACIÓN DE LA INVENCIÓN

Por lo tanto, existe una necesidad de nuevos sistemas, procedimientos y productos de programa informático para realizar operaciones criptográficas de forma centralizada, pero que ofrezcan un mejor equilibrio entre las capacidades de centralización y las capacidades de seguridad en los términos descritos anteriormente.

El objeto de la presente invención es el de satisfacer dicha necesidad. Dicho objeto se consigue con un procedimiento según la reivindicación 1, un procedimiento según la reivindicación 12, un producto de programa informático según la reivindicación 14, un procedimiento según la reivindicación 17, un producto de programa informático según la reivindicación 19, un sistema según la reivindicación 20, un sistema informático cliente según la reivindicación 21, un sistema informático servidor según la reivindicación 22, un sistema según la reivindicación 23, un sistema informático cliente según la reivindicación 24, y un sistema informático servidor según la reivindicación 25.

En un primer aspecto, la presente invención proporciona un procedimiento de proporcionar un resultado de una operación criptográfica desde un sistema informático servidor, comprendiendo dicho procedimiento: recibir, por parte del sistema informático servidor, que comprende un gestor de múltiples repositorios y al menos un repositorio de claves criptográficas remotas, una petición de usuario de la operación criptográfica procedente de un sistema informático cliente; obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas; establecer, por parte del gestor de múltiples repositorios, una clave criptográfica referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica; solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el cual está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota; obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica; y enviar, por parte del sistema informático servidor, el resultado de la operación criptográfica al sistema informático cliente.

El concepto "sistema informático cliente" en el contexto de la presente invención debe entenderse como un sistema informático que comprende medios para solicitar operaciones criptográficas a otro sistema informático y medios para recibir los resultados de las operaciones criptográficas procedentes de dicho otro sistema informático. Y el concepto "sistema informático servidor" debe ser entendido como un sistema informático que comprende medios para recibir solicitudes de operaciones criptográficas, medios para realizar dichas operaciones criptográficas y medios para devolver los resultados de las operaciones criptográficas realizadas a "sistemas informáticos cliente". Así, por ejemplo, un sistema informático que actúa como un servidor de otros servicios, por ejemplo, un servidor web, puede ser un "sistema informático cliente" en el contexto de la presente invención, y un sistema informático que actúa como un cliente de otros servicios, por ejemplo, un cliente web, puede ser un "sistema informático servidor" en el contexto de la presente invención.

El significado del término "sistema" puede referirse a un conjunto de elementos de hardware, como por ejemplo un conjunto de ordenadores, que comprende los medios necesarios para la interacción entre ellos. Por ejemplo, el "sistema informático servidor" puede comprender un primer ordenador que comprende el gestor de múltiples repositorios y un segundo ordenador que comprende el al menos un repositorio de claves criptográficas, estando dichos primer y segundo ordenadores conectados entre sí de tal manera que dichos primer y segundo ordenadores pueden interactuar de forma conveniente.

El procedimiento de proporcionar un resultado de una operación criptográfica desde un sistema informático servidor, y en particular la provisión del gestor de múltiples repositorios y su papel en dicho procedimiento, permite tener almacenada cada clave criptográfica en un repositorio adecuado, de tal forma que dicho repositorio puede ofrecer las capacidades de seguridad estrictamente necesarias según la criticidad de las claves que se almacenan en dicho repositorio. Así, por ejemplo, en el caso de una empresa que tiene claves criptográficas de dos categorías de criticidad (por ejemplo críticas y no críticas), se puede utilizar un repositorio de alta seguridad (por ejemplo, un HSM) para almacenar las claves críticas y se puede utilizar una base de datos convencional para almacenar las claves que no son críticas.

Con esta configuración, todas las claves de la empresa pueden ser almacenadas y utilizadas de forma centralizada en dichos repositorios diferentes, los cuales son gestionados de forma centralizada por el gestor de múltiples repositorios. Además, se proporcionan capacidades de seguridad particulares para cada clave almacenada en

función del repositorio en el que está almacenada la clave, de tal manera que, por ejemplo, el HSM del ejemplo anterior se puede dimensionar de acuerdo a la cantidad de claves críticas de la empresa y, por lo tanto, se puede optimizar el coste de almacenar de forma centralizada todas las claves (críticas y no críticas) de la empresa, ya que se evita el almacenamiento de claves no críticas en un costoso HSM.

Además, como el gestor de múltiples repositorios tiene la capacidad de gestionar diferentes tipos de repositorios, un repositorio actual puede ser fácilmente sustituido por otro tipo de repositorio seguro con un impacto muy bajo en el funcionamiento normal de los sistemas de la empresa. En el caso de que el gestor de múltiples repositorios todavía no soporte el nuevo repositorio seguro a integrar en los sistemas de la empresa, sólo será necesario desarrollar un nuevo módulo para interactuar con dicho nuevo repositorio como una parte nueva del gestor de múltiples repositorios, por lo que incluso en este caso, el impacto de esta evolución en el funcionamiento normal de los sistemas de la empresa será todavía bastante bajo.

Por lo tanto, teniendo en cuenta las argumentaciones anteriores, se puede concluir que este procedimiento de proporcionar un resultado de una operación criptográfica desde un sistema informático servidor permite tener una flexibilidad muy alta que permite evoluciones potenciales más baratas de los sistemas de la empresa (por ejemplo, en el sistema informático servidor), tanto en términos de requerir repositorios seguros dimensionados convenientemente y, por lo tanto, sin capacidades de seguridad innecesarias y costosas, como en términos de adaptaciones de bajo impacto en los sistemas actuales para la integración de un nuevo repositorio de certificados.

En un segundo aspecto de la presente invención, se proporciona un producto de programa informático que comprende instrucciones de programa para hacer que un ordenador realice el procedimiento de proporcionar un resultado de una operación criptográfica desde un sistema informático servidor. La invención también se refiere a dicho producto de programa informático incluido en un medio de almacenamiento (por ejemplo, un CD-ROM, un DVD, una unidad USB, en una memoria de ordenador o en una memoria de sólo lectura) o portado por una señal portadora (por ejemplo, una señal portadora eléctrica u óptica).

Según un tercer aspecto de la invención, se proporciona un sistema informático servidor para proporcionar un resultado de una operación criptográfica, comprendiendo el sistema informático servidor un gestor de múltiples repositorios, al menos un repositorio de claves criptográficas remotas, un procesador y una memoria; en el que la memoria del sistema informático servidor almacena instrucciones ejecutables por ordenador que, cuando son ejecutadas, hacen que el sistema informático servidor realice un procedimiento que comprende: recibir, por parte del sistema informático servidor, una petición de usuario de la operación criptográfica procedente de un sistema informático cliente; obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas; establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica; solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota; obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica; y enviar, por parte del sistema informático servidor, el resultado de la operación criptográfica al sistema informático cliente.

En un cuarto aspecto de la presente invención, se proporciona un sistema informático servidor para proporcionar un resultado de una operación criptográfica, que comprende: medios informáticos para recibir una petición de usuario de la operación criptográfica procedente de un sistema informático cliente; medios informáticos para enviar el resultado de la operación criptográfica al sistema informático cliente; al menos un repositorio de claves criptográficas remotas; y un gestor de múltiples repositorios. Comprendiendo dicho gestor de múltiples repositorios: medios informáticos para obtener un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas; medios informáticos para establecer una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica; medios informáticos para solicitar la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota; y medios informáticos para obtener el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica.

El producto de programa informático del segundo aspecto, el sistema informático servidor del tercer aspecto, y el sistema informático servidor del cuarto aspecto de la invención son adecuados para llevar a cabo el procedimiento de proporcionar un resultado de una operación criptográfica desde un sistema informático servidor, habiendo sido dicho procedimiento comentado previamente como el primer aspecto de la invención. Por lo tanto, todas las ventajas

y principios comentados en relación con dicho procedimiento (primer aspecto de la invención) también son atribuibles a dicho producto de programa informático (segundo aspecto de la invención), y a dichos dos sistemas informáticos servidores (aspectos tercero y cuarto de la invención).

Según un quinto aspecto de la invención, se proporciona un procedimiento de obtención de un resultado de una operación criptográfica en un sistema informático cliente, comprendiendo dicho procedimiento: enviar, por parte del sistema informático cliente, una petición de usuario de la operación criptográfica a un sistema informático servidor que comprende un gestor de múltiples repositorios y al menos un repositorio de claves criptográficas remotas; y recibir, por parte del sistema informático cliente, el resultado de la operación criptográfica procedente del sistema informático servidor, en el que dicho resultado de la operación criptográfica recibido es el resultado de: obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas; establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica; solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota; y obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica.

Este procedimiento de obtención de un resultado de una operación criptográfica en un sistema informático cliente permite a dicho sistema informático cliente la obtención del resultado de la operación criptográfica de tal manera que todas las ventajas y principios comentados en relación con el procedimiento de proporcionar un resultado de una operación criptográfica desde un sistema informático servidor (primer aspecto de la invención) son también de consideración en este caso.

En un sexto aspecto de la presente invención, se proporciona un producto de programa informático que comprende instrucciones de programa para hacer que un ordenador realice el procedimiento de obtención de un resultado de una operación criptográfica en un sistema informático cliente. La invención también se refiere a dicho producto de programa informático incluido en un medio de almacenamiento (por ejemplo, un CD-ROM, un DVD, una unidad USB, en una memoria de ordenador o en una memoria de sólo lectura) o portado por una señal portadora (por ejemplo, una señal portadora eléctrica u óptica).

Según un séptimo aspecto de la presente invención, se proporciona un sistema informático cliente para obtener un resultado de una operación criptográfica en el sistema informático cliente, comprendiendo el sistema informático cliente un procesador y una memoria; en el que la memoria del sistema informático cliente almacena instrucciones ejecutables por ordenador que, cuando son ejecutadas, hacen que el sistema informático cliente realice un procedimiento que comprende: enviar, por parte del sistema informático cliente, una petición de usuario de la operación criptográfica a un sistema informático servidor que comprende un gestor de múltiples repositorios y al menos un repositorio de claves criptográficas remotas; y recibir, por parte del sistema informático cliente, el resultado de la operación criptográfica procedente del sistema informático servidor. Siendo dicho resultado de la operación criptográfica recibido el resultado de: obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas; establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica; solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota; y obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica.

En un octavo aspecto de la presente invención, se proporciona un sistema informático cliente para obtener un resultado de una operación criptográfica en el sistema informático cliente, que comprende: medios informáticos para enviar una petición de usuario de la operación criptográfica a un sistema informático servidor que comprende un gestor de múltiples repositorios y al menos un repositorio de claves criptográficas remotas; y medios informáticos para recibir el resultado de la operación criptográfica procedente del sistema informático servidor. Siendo dicho resultado de la operación criptográfica recibido el resultado de: obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas; establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica; solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave

criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota; y obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica.

El producto de programa informático del sexto aspecto, el sistema informático cliente del séptimo aspecto, y el sistema informático cliente del octavo aspecto de la invención son adecuados para llevar a cabo el procedimiento de obtención de un resultado de una operación criptográfica en un sistema informático cliente, habiendo sido dicho procedimiento comentado previamente como el quinto aspecto de la invención. Por lo tanto, todas las ventajas y principios considerados con respecto a dicho procedimiento (quinto aspecto de la invención) también son atribuibles a dicho producto de programa informático (sexto aspecto de la invención), y a dichos dos sistemas informáticos cliente (aspectos séptimo y octavo de la invención).

Según la presente invención, se proporciona un procedimiento de realizar una operación criptográfica, comprendiendo dicho procedimiento: enviar por parte de un sistema informático cliente una petición de usuario de la operación criptográfica a un sistema informático servidor que comprende un gestor de múltiples repositorios y al menos un repositorio de claves criptográficas remotas; obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas; establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica; solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota; obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica; y enviar, por parte del sistema informático servidor, el resultado de la operación criptográfica al sistema informático cliente.

Según la presente invención, se proporciona un sistema para realizar una operación criptográfica, que comprende al menos un sistema informático cliente y un sistema informático servidor; en el que el sistema informático servidor comprende un gestor de múltiples repositorios, al menos un repositorio de claves criptográficas remotas, un procesador y una memoria; en el que el sistema informático cliente comprende un procesador y una memoria; y en el que la memoria del sistema informático servidor y la memoria del sistema informático cliente almacenan instrucciones ejecutables por ordenador que, cuando son ejecutadas, hacen que los sistemas informáticos servidor y cliente realicen un procedimiento que comprende: enviar, por parte del sistema informático cliente, una petición de usuario de la operación criptográfica al sistema informático servidor; obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas; establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica; solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota; obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica; y enviar, por parte del sistema informático servidor, el resultado de la operación criptográfica al sistema informático cliente.

Según la presente invención, se proporciona un sistema para realizar una operación criptográfica, que comprende al menos un sistema informático cliente y un sistema informático servidor. Comprendiendo el sistema informático cliente: medios informáticos para enviar una petición de usuario de la operación criptográfica al sistema informático servidor; y medios informáticos para recibir el resultado de la operación criptográfica procedente del sistema informático servidor. Comprendiendo el sistema informático servidor: medios informáticos para recibir la petición de usuario de la operación criptográfica procedente del sistema informático cliente; medios informáticos para enviar el resultado de la operación criptográfica al sistema informático cliente; al menos un repositorio de claves criptográficas remotas; y un gestor de múltiples repositorios. Comprendiendo el gestor de múltiples repositorios: medios informáticos para obtener un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas; medios informáticos para establecer una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica; medios informáticos para solicitar la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota; y medios informáticos para obtener el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica.

A lo largo de la descripción y las reivindicaciones la palabra "comprende" y variaciones de la palabra, no pretenden

excluir otras características técnicas, aditivos, componentes o etapas. Objetos, ventajas y características adicionales de la invención serán evidentes para los expertos en la técnica tras el examen de la descripción o se pueden aprender mediante la práctica de la invención. Los siguientes ejemplos y dibujos se proporcionan a modo de ilustración, y no se pretende que sean limitativos de la presente invención. Los signos de referencia relacionados con los dibujos y colocados entre paréntesis en una reivindicación, son únicamente para tratar de aumentar la inteligibilidad de la reivindicación, y no deberán interpretarse como limitativos del alcance de la reivindicación. Además, la presente invención cubre todas las posibles combinaciones de realizaciones particulares y preferidas descritas en el presente documento.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

A continuación se describirán realizaciones particulares de la presente invención por medio de ejemplos no limitativos, con referencia a los dibujos adjuntos, en los que:

La figura 1 es una representación esquemática de un sistema para realizar operaciones criptográficas, según una realización de la invención.

EXPOSICION DETALLADA DE MODOS DE REALIZACIÓN

En las siguientes descripciones, se exponen numerosos detalles específicos con el fin de proporcionar una comprensión completa de la presente invención. Se entenderá, sin embargo, por parte de un experto en la técnica, que la presente invención puede ponerse en práctica sin algunos o todos de estos detalles específicos. En otros casos, no se han descrito en detalle elementos bien conocidos para no oscurecer innecesariamente la descripción de la presente invención.

La figura 1 representa una realización del sistema para llevar a cabo operaciones criptográficas, comprendiendo dicha realización al menos un sistema informático cliente 100 y un sistema informático servidor 101 conectados a través de una red de comunicaciones 113.

El sistema informático servidor 101 puede comprender:
- un gestor de múltiples repositorios 106;
- un primer repositorio 107 de claves criptográficas remotas;
- un segundo repositorio 108 de claves criptográficas remotas;
- un módulo de contexto de uso 109;
- un repositorio de reglas de contexto de uso 110;
- un módulo de eventos criptográficos 111;
- un repositorio de eventos criptográficos 112;
- un procesador (no mostrado); y
- una memoria (no mostrada).

El gestor de múltiples repositorios 106 puede estar adaptado para recibir datos (por ejemplo, peticiones de operaciones criptográficas) procedentes de un módulo cliente 103 del sistema informático cliente 100, para interactuar con el primer repositorio 107 y el segundo repositorio 108 de claves criptográficas remotas para por ejemplo realizar operaciones criptográficas solicitadas, y para enviar datos (por ejemplo, los resultados de las operaciones criptográficas realizadas) al módulo cliente 103.

El intercambio de datos entre el módulo cliente 103 y el gestor de múltiples repositorios 106 a través de la red de comunicaciones 113 se puede realizar estructurando dichos datos según una estructura adecuada independiente de repositorio, empaquetando de forma conveniente dichos datos estructurados independientes de repositorio por razones de eficiencia en las transmisiones, y usando un canal seguro (por ejemplo, un canal SSL) por razones de seguridad en las transmisiones. Así, por ejemplo, el módulo cliente 103 puede enviar datos de peticiones de operaciones criptográficas estructurados bajo dicha estructura adecuada independiente de repositorio y empaquetados bajo una estructura adecuada de empaquetado y usando dicho canal SSL. De igual manera, el gestor de múltiples repositorios 106 puede enviar datos de resultados de operaciones criptográficas estructurados bajo dicha estructura adecuada independiente de repositorio y empaquetados bajo dicha estructura adecuada de empaquetado y utilizando dicho canal SSL.

Por lo tanto, dicho intercambio de datos estructurados bajo dicha estructura adecuada independiente de repositorio puede ser entendido como que el módulo cliente 103 y el gestor de múltiples repositorios 106 usan un lenguaje único independiente de repositorio para comunicarse entre ellos.

El gestor de múltiples repositorios 106 puede comprender un módulo independiente de repositorio para recibir datos empaquetados procedentes del módulo cliente 103 y para desempaquetar dichos datos una vez recibidos, teniendo dichos datos desempaquetados la estructura independiente de repositorio comentada anteriormente. El gestor de múltiples repositorios 106 puede comprender además un módulo dependiente de repositorio para cada tipo de entre una pluralidad de diferentes tipos de repositorios de claves criptográficas, siendo el primer repositorio 107 y el segundo repositorio 108 de uno de dichos tipos de repositorios, de tal de manera que uno de los módulos dependientes de repositorio está adaptado para interactuar con el primer repositorio 107 y uno de los módulos dependientes de repositorio está adaptado para interactuar con el segundo repositorio 108.

Cada uno de los módulos dependientes de repositorio puede estar adaptado para obtener datos desempaquetados del módulo independiente de repositorio, y transformar dichos datos desempaquetados en correspondientes instrucciones para su ejecución en el correspondiente repositorio de claves criptográficas. Igualmente, cada uno de dichos módulos dependientes de repositorio puede estar adaptado para obtener datos producidos en el repositorio de claves criptográficas correspondiente, y para transformar dichos datos obtenidos en la estructura independiente de repositorio comentada previamente. El módulo independiente de repositorio puede estar adaptado, además, para obtener datos de los módulos dependientes de repositorio, estando dichos datos estructurados bajo la estructura independiente de repositorio, para empaquetar dichos datos obtenidos bajo la estructura adecuada de empaquetado, y para enviar dichos datos empaquetados al módulo cliente 103.

Las funcionalidades descritas anteriormente con respecto a los módulos dependientes de repositorio pueden ser entendidas como que el gestor de múltiples repositorios 106 utiliza un lenguaje dependiente de repositorio para interactuar con cada tipo diferente de repositorio de claves criptográficas (primer repositorio 107 y segundo repositorio 108 en la realización de la figura 1). Por lo tanto, la configuración del gestor de múltiples repositorios 106 basada en el módulo independiente de repositorio y los módulos dependientes de repositorio permite la integración de nuevos tipos de repositorios con un impacto muy bajo en el sistema.

El primer repositorio 107 puede ser un HSM de alta seguridad para el almacenamiento de claves de criticidad alta, mientras que el segundo repositorio 108 puede ser una base de datos convencional para el almacenamiento de claves de criticidad baja. Sin embargo, el sistema informático servidor 101 puede comprender otros repositorios de claves criptográficas remotas en función de los diferentes niveles de criticidad de las claves criptográficas remotas existentes. Por ejemplo, el sistema informático servidor 101 podría comprender un tercer repositorio para el almacenamiento de claves de criticidad media.

El módulo de contexto de uso 109 puede estar adaptado para interactuar con el gestor de múltiples repositorios 106 para la determinación de claves criptográficas remotas permitidas para el usuario de solicitudes recibidas de operaciones criptográficas, siendo dicha determinación de claves permitidas de acuerdo con el contenido del repositorio de reglas de contexto de uso 110. El concepto de "contexto de uso" se refiere a las condiciones de contexto bajo las cuales se ha solicitado una operación criptográfica y a la autorización o denegación del uso de una clave criptográfica remota concreta en función de dichas condiciones contextuales.

El módulo de eventos criptográficos 111 puede estar adaptado para almacenar en el repositorio de eventos criptográficos 112 datos relacionados con cualquier tipo de eventos criptográficos producidos en el sistema informático servidor 101 para, por ejemplo, su inspección posterior. Dichos datos relacionados con eventos criptográficos pueden comprender datos relacionados con resultados de operaciones criptográficas obtenidos por el gestor de múltiples repositorios 106, datos relativos a solicitudes recibidas por el gestor de múltiples repositorios 106, etc.

La memoria del sistema informático servidor 101 puede almacenar un programa informático que comprende instrucciones ejecutables que, cuando son ejecutadas por el procesador, hacen que el sistema informático servidor 101 realice un procedimiento para proporcionar un resultado de una operación criptográfica, comprendiendo dicho procedimiento:

- recibir, por parte del gestor de múltiples repositorios 106, una petición de usuario de la operación criptográfica procedente del módulo cliente 103;
- obtener, por parte del gestor de múltiples repositorios 106, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del primer 107 y segundo 108 repositorios de claves criptográficas remotas;
- establecer, por parte del gestor de múltiples repositorios 106, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica;
- solicitar, por parte del gestor de múltiples repositorios 106, la realización de la operación criptográfica al repositorio (primero 107 o segundo 108) en el que está almacenada la clave criptográfica remota a utilizar, para que dicha

operación criptográfica sea realizada usando dicha clave criptográfica remota;
• obtener, por parte del gestor de múltiples repositorios 106, el resultado de la operación criptográfica procedente del repositorio (primero 107 o segundo 108) de claves criptográficas remotas que ha realizado la operación criptográfica;
• enviar, por parte del gestor de múltiples repositorios 106, el resultado de la operación criptográfica al módulo cliente 103.

En el contexto descrito en el párrafo anterior, el gestor de múltiples repositorios 106, el módulo de contexto de uso 109 y el módulo de eventos criptográficos 111 pueden ser sub-módulos (por ejemplo, subrutinas) del programa informático almacenado en la memoria del sistema informático servidor 101.

El sistema informático cliente 100 puede comprender:
• un módulo cliente 103;
• un repositorio local 104 adaptado para almacenar claves criptográficas locales;
• un procesador (no mostrado); y
• una memoria (no mostrada).

El módulo cliente 103 puede estar adaptado para capturar solicitudes de operaciones criptográficas procedentes de una o más aplicaciones 102 que se ejecutan en el sistema informático cliente 100, para enviar cada solicitud capturada al gestor de múltiples repositorios 106, y para recibir cada resultado de las operaciones criptográficas ejecutadas procedentes del gestor de múltiples repositorios 106.

La memoria del sistema informático cliente 100 puede almacenar un programa informático que comprende instrucciones ejecutables que, cuando son ejecutadas por el procesador, hacen que el sistema informático cliente realice un procedimiento de obtención de un resultado de una operación criptográfica, comprendiendo dicho procedimiento:
• enviar por parte del módulo cliente 103, que puede ser un sub-módulo (por ejemplo, una subrutina) de dicho programa informático del cliente, la petición de usuario de la operación criptográfica al gestor de múltiples repositorios 106;
• recibir, por parte del módulo cliente 103, el resultado de la operación criptográfica procedente del gestor de múltiples repositorios 106, siendo dicho resultado recibido el resultado de la operación criptográfica obtenido por el gestor de múltiples repositorios 106, según se describió anteriormente.

En consecuencia, la forma de realización del sistema mostrada en la figura 1 puede realizar un procedimiento de realizar una operación criptográfica que comprende:
• enviar, por parte del módulo cliente 103, una petición de usuario de la operación criptográfica al gestor de múltiples repositorios 106;
• obtener, por parte del gestor de múltiples repositorios 106, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del primer 107 y segundo 108 repositorios de claves criptográficas remotas;
• establecer, por parte del gestor de múltiples repositorios 106, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica;
• solicitar, por parte del gestor de múltiples repositorios 106, la realización de la operación criptográfica al repositorio (primero 107 o segundo 108) en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota;
• obtener, por parte del gestor de múltiples repositorios 106, el resultado de la operación criptográfica procedente del repositorio (primero 107 o segundo 108) de claves criptográficas remotas que ha realizado la operación criptográfica;
• enviar, por parte del gestor de múltiples repositorios 106, el resultado de la operación criptográfica al módulo cliente 103.

Preferiblemente, el procedimiento de realizar una operación criptográfica puede comprender además:
• enviar, por parte del gestor de múltiples repositorios 106, el conjunto obtenido de referencias a claves criptográficas remotas al módulo cliente 103;
• seleccionar, por parte del módulo cliente 103, una referencia del conjunto de referencias a claves criptográficas remotas según una petición de usuario para la selección de claves criptográficas remotas;
• enviar, por parte del módulo cliente 103, la referencia a clave criptográfica remota seleccionada al gestor de múltiples repositorios 106;
y en el que establecer, por parte del gestor de múltiples repositorios 106, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica comprende:
• establecer, por parte del gestor de múltiples repositorios 106, la clave criptográfica remota referenciada por la referencia a clave criptográfica remota seleccionada, recibida procedente del módulo cliente 103, como la clave

criptográfica remota a utilizar para la realización de la operación criptográfica.

Alternativamente a los criterios de selección de la clave remota descritos en el párrafo anterior, cada clave criptográfica remota almacenada puede comprender una prioridad, de manera que el gestor de múltiples repositorios puede establecer la clave criptográfica remota a utilizar para la realización de la operación criptográfica mediante la selección de la clave con la prioridad más alta del conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario.

Como alternativa a los criterios de selección de la clave remota descritos en los dos párrafos anteriores, cada clave criptográfica remota almacenada puede comprender una fecha de fin de validez, de manera que el gestor de múltiples repositorios puede establecer la clave criptográfica remota a utilizar para la realización de la operación criptográfica seleccionando la clave con la fecha de fin de validez más lejana del conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario.

En algunas formas de realización de la invención, el procedimiento de realizar una operación criptográfica puede comprender además:
• obtener, por parte del módulo cliente 103, un conjunto de referencias a claves criptográficas locales permitidas para la petición de usuario del repositorio local 104;
• establecer, por parte del módulo cliente 103, una clave criptográfica local referenciada en el conjunto de referencias a claves criptográficas locales como la clave criptográfica local a utilizar para la realización de la operación criptográfica;
• realizar, por parte del módulo cliente 103, la operación criptográfica usando la clave criptográfica local a utilizar para la realización de la operación criptográfica.

Preferiblemente, el procedimiento de realizar una operación criptográfica puede comprender además:
• seleccionar, por parte del módulo cliente 103, una referencia del conjunto de referencias a claves criptográficas locales según una petición de usuario para la selección de claves criptográficas locales;
y en el que establecer, por parte del módulo cliente 103, una clave criptográfica local referenciada en el conjunto de referencias a claves criptográficas locales como la clave criptográfica local a utilizar para la realización de la operación criptográfica comprende:
• establecer, por parte del módulo cliente 103, una clave criptográfica local referenciada por la referencia a clave criptográfica local seleccionada como la clave criptográfica local a utilizar para la realización de la operación criptográfica.

Alternativamente a los criterios de selección de la clave local descritos en el párrafo anterior, cada clave criptográfica local almacenada puede comprender una prioridad, de manera que el módulo cliente puede establecer la clave criptográfica local a utilizar para la realización de la operación criptográfica seleccionando la clave con la prioridad más alta del conjunto de referencias a claves criptográficas locales permitidas para la petición de usuario.

Alternativamente a los criterios de selección de la clave local descritos en los dos párrafos anteriores, cada clave criptográfica local almacenada puede comprender una fecha de fin de validez, de modo que el módulo cliente 103 puede establecer la clave criptográfica local a utilizar para la realización de la operación criptográfica mediante la selección de la clave con la fecha de fin de validez más lejana del conjunto de referencias a claves criptográficas locales permitidas para la petición de usuario.

Dando el sistema la opción al usuario de utilizar también claves locales para llevar a cabo operaciones criptográficas ofrece una gran flexibilidad al sistema y los procedimientos relacionados, ya que, por ejemplo, la integración de un nuevo repositorio en el sistema puede requerir que algunas claves sean almacenadas localmente temporalmente en los sistemas informáticos cliente durante un cierto período de tiempo, mientras que, por ejemplo, no se haya integrado definitivamente el nuevo repositorio en el sistema. En otras palabras, el uso de claves almacenadas localmente puede ser especialmente ventajoso durante la transición desde una situación en la que dicho nuevo repositorio no ha sido implantado hasta una situación en la que dicho nuevo repositorio ha sido implantado.

En formas de realización de la invención, el gestor de múltiples repositorios 106 puede determinar que una clave criptográfica remota está permitida para la petición de usuario cuando dicha clave criptográfica remota y la petición de usuario se corresponden con una regla de contexto de uso almacenada en el repositorio de reglas de contexto de uso 110, y dicha regla de contexto de uso correspondida comprende una acción resultante que indica que está permitido el uso de la clave criptográfica remota.

El uso de reglas de contexto de uso constituye una herramienta muy potente para tener en cuenta políticas corporativas generales con respecto a la utilización de determinados tipos de certificados. Por ejemplo, si la empresa determina que los ingenieros pueden utilizar determinados tipos de certificados (por ejemplo, claves para la firma de

documentos técnicos) sólo durante determinados períodos de tiempo (por ejemplo, entre las 09:00 h y las 18:00 h), esta política puede ser implantada muy fácilmente mediante la creación de una nueva regla de contexto de uso o modificando una regla de contexto de uso existente que refleje dicha lógica. Por lo tanto, se puede concluir que el uso de reglas de contexto de uso añade aún más flexibilidad al sistema y procedimientos relacionados.

En formas de realización de la invención, cada regla de contexto de uso almacenada en el repositorio de reglas de contexto de uso 110 puede comprender, además, un perfil de usuario y un perfil de clave criptográfica, y el gestor de múltiples repositorios 106 puede determinar que una clave criptográfica remota y la petición de usuario se corresponden con una regla de contexto de uso cuando el usuario de la petición de usuario pertenece al perfil de usuario de dicha regla de contexto de uso y dicha clave criptográfica remota pertenece al perfil de la clave criptográfica de dicha regla de contexto de uso.

Por ejemplo, suponiendo la petición de operación criptográfica, el conjunto de claves criptográficas potencialmente aplicables y la regla de contexto de uso indicadas en la Tabla 1, se establecerá la clave K2 como la clave a utilizar para realizar la operación criptográfica, ya que la regla de contexto de uso existente 'claves del perfil KP2 están permitidas para los usuarios del perfil UP1' se corresponde con la petición (perfil de usuario = UP1) y la clave K2 (perfil de clave = KP2) y dicha regla correspondida permite el uso de la clave (acción resultante = permitida).

Petición de operación criptográfica	Realizada por un usuario U1 que pertenece al perfil de usuario UP1
Conjunto de claves criptográficas aplicables potencialmente	K1 que pertenece al perfil KP1 K2 que pertenece al perfil KP2
Reglas de contexto de uso existentes	'claves del perfil KP2 se permiten para usuarios del perfil UP1', en la que 'claves del perfil KP2' se refiere al parámetro perfil de clave criptográfica, 'usuarios del perfil UP1' se refiere al parámetro perfil de usuario y 'se permiten' se refiere a la acción resultante

Tabla 1

Ejemplos de perfiles de usuario pueden ser:
INGENIEROS - empleados de la empresa que son ingenieros
SISTEMAS - empleados de la empresa que son técnicos de sistemas

Ejemplos de perfiles de claves criptográficas pueden ser:
INTRANET - claves de acceso a la intranet de la empresa
APROBACIÓN - claves para firmar la aprobación de un documento interno

En algunas realizaciones, cada regla de contexto de uso almacenada en el repositorio de reglas de contexto de uso 110 puede comprender, además, un perfil de condiciones técnicas, y el gestor de múltiples repositorios 106 puede determinar que una clave criptográfica remota y la petición de usuario se corresponden con una regla de contexto de uso cuando el usuario de la petición de usuario pertenece al perfil de usuario de dicha regla de contexto de uso, dicha clave criptográfica remota pertenece al perfil de clave criptográfica de dicha regla de contexto de uso, y las condiciones técnicas bajo las que se ha realizado la petición de usuario pertenecen al perfil de condiciones técnicas de la citada regla de contexto de uso.

El perfil de condiciones técnicas puede referirse a al menos uno de los siguientes parámetros: la hora de la petición de usuario (es decir, hora en la que se ha hecho la petición de usuario), el perfil del sistema informático cliente (por ejemplo, dispositivo móvil, dispositivo de red corporativa, etc.), la ubicación del sistema informático cliente (por ejemplo, dentro o fuera de la red corporativa), y el perfil de la aplicación a través de la que se ha efectuado la petición de usuario (por ejemplo, Office, Acrobat, etc.).

Por ejemplo, suponiendo la petición de operación criptográfica, el conjunto de claves criptográficas potencialmente aplicables y la regla de contexto de uso existente indicadas en la Tabla 2, la clave K1 será establecida como la clave a utilizar para realizar la operación criptográfica, porque sólo la regla de contexto de uso 'claves del perfil KP1 están permitidas para usuarios del perfil UP1 entre las 09:00 h y las 18:00 h' se corresponde con la solicitud (perfil de usuario = UP1 y '10: 31h' está entre 'las 09:00 h y las 18:00 h') y la clave K1 (perfil de clave = KP1), y dicha regla correspondida permite el uso de la clave (acción resultante = permitida).

Petición de operación criptográfica	Realizada por el usuario U1 que pertenece al perfil de usuario UP1 Realizada a las 10:31h
Conjunto de claves	K1 que pertenece al perfil KP1

criptográficas potencialmente aplicables	K2 que pertenece al perfil KP2
Reglas de contexto de uso existentes	‘claves del perfil KP2 se permiten para usuarios del perfil UP1 entre 13:00h y 18:00h' ‘claves del perfil KP1 se permiten para usuarios del perfil UP1 entre 09:00h y 18:00h'

Tabla 2

En algunas formas de realización, cada regla de contexto de uso almacenada en el repositorio de reglas de contexto de uso 110 puede comprender además una prioridad, y el gestor de múltiples repositorios 106 puede determinar que se permite una clave criptográfica remota para la petición de usuario cuando dicha clave criptográfica remota y la petición de usuario se corresponden con al menos una regla de contexto de uso y la regla de contexto de uso de dicha al menos una regla de contexto de uso correspondida que tiene la prioridad más alta comprende una acción resultante que indica que se permite utilizar la clave criptográfica remota.

Por ejemplo, suponiendo la petición de operación criptográfica, el conjunto de claves criptográficas potencialmente aplicables y las reglas de contexto de uso existentes que se indican en la Tabla 3, la clave K1 será establecida como la clave a utilizar para realizar la operación criptográfica, porque:

la regla de contexto de uso ‘claves del perfil KP1 no están permitidas para los usuarios del perfil UP1 entre las 13:00 h y las 18:00 h' se corresponde con la solicitud (perfil de usuario = UP1 y '13: 31h' está entre 'las 09:00 h y las 18:00 h') y la clave K1 (perfil de clave = KP1), no permitiendo dicha regla correspondida el uso de la clave (acción resultante = no permitida);

la regla de contexto de uso ‘claves del perfil KP1 están permitidas para los usuarios del perfil UP1 entre las 09:00 h y las 18:00 h' se corresponde con la solicitud (perfil de usuario = UP1 y '13:31 h' está entre 'las 09:00 h y las 18:00 h') y la clave K1 (perfil de clave = KP1), permitiendo dicha regla correspondida el uso de la clave (acción resultante = permitida);

pero la prioridad de la regla que permite el uso de la clave (prioridad 20) es mayor que la prioridad de la regla que no permite el uso de la clave (prioridad 10), por lo que la regla de prioridad 20 prevalece frente a la regla de prioridad 10, por lo que el uso de la clave K1 está permitido según la regla 'claves del perfil KP1 están permitidas para los usuarios del perfil UP1 entre las 09:00 h y las 18:00 h'.

Petición de operación criptográfica	Realizada por un usuario U1 que pertenece al perfil de usuario UP1 Realizada a las 13:31h
Conjunto de claves criptográficas potencialmente aplicables	K1 que pertenece al perfil KP1 K2 que pertenece al perfil KP2
Reglas de contexto de uso existentes	‘claves del perfil KP1 no están permitidas para usuarios del perfil UP1 entre 13:00h y 18:00h' - prioridad 10 ‘claves del perfil KP1 están permitidas para usuarios del perfil UP1 entre 09:00h y 18:00h' - prioridad 20

Tabla 3

Aunque esta invención se ha descrito en el contexto de ciertas realizaciones y ejemplos preferidos, se entenderá por parte de los expertos en la técnica que la presente invención se extiende más allá de las realizaciones divulgadas específicamente a otras formas de realización y/o usos alternativos de la invención y modificaciones obvias y equivalentes de las mismas. Por lo tanto, se pretende que el alcance de la presente invención divulgada en este documento no se limite a las formas de realización particulares divulgadas descritas anteriormente, sino que se debería determinar sólo por una lectura razonable de las reivindicaciones que siguen.

Además, aunque las formas de realización de la invención descritas con referencia a los dibujos comprenden aparatos y procesos realizados en un aparato informático, la invención se extiende también a programas informáticos, en particular a programas informáticos en un portador, adaptados para poner en práctica la invención. El programa puede ser en forma de código fuente, código objeto, un código intermedio entre código fuente y código objeto tal como en una forma compilada parcialmente, o en cualquier otra forma adecuada para su uso en la implementación de los procesos según la invención. El portador puede ser cualquier entidad o dispositivo capaz de portar el programa.

Por ejemplo, el portador puede comprender un medio de almacenamiento, tal como una ROM, por ejemplo un CD ROM o una ROM de semiconductores, o un medio de grabación magnética, por ejemplo un disquete o disco duro. Además, el portador puede ser un portador transmisible tal como una señal eléctrica u óptica, que puede ser

transmitida a través de cable eléctrico u óptico o por radio u otros medios.

Cuando el programa está incluido en una señal que puede ser transportada directamente por un cable u otro dispositivo o medio, el portador puede estar constituido por dicho cable u otro dispositivo o medio.

Alternativamente, el portador puede ser un circuito integrado en el cual está integrado el programa, estando el circuito integrado adaptado para realizar, o para su uso en la realización de, los procesos relevantes.

REIVINDICACIONES

1. Procedimiento de realización de una operación criptográfica, que comprende:
• enviar por parte de un sistema informático cliente una petición de usuario de la operación criptográfica a un sistema informático servidor que comprende un gestor de múltiples repositorios y al menos un repositorio de claves criptográficas remotas;
• obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas;
• establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica;
• solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota;
• obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica;
• enviar, por parte del sistema informático servidor, el resultado de la operación criptográfica al sistema informático cliente.

2. Procedimiento según la reivindicación 1, que comprende además:
• enviar, por parte del sistema informático servidor, el conjunto obtenido de referencias a claves criptográficas remotas al sistema informático cliente;
• seleccionar, por parte del sistema informático cliente, una referencia del conjunto de referencias a claves criptográficas remotas según una petición de usuario para la selección de claves criptográficas remotas;
• enviar, por parte del sistema informático cliente, la referencia a clave criptográfica remota seleccionada al sistema informático servidor;
y en el que establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica comprende:
• establecer, por parte del gestor de múltiples repositorios, la clave criptográfica remota referenciada por la referencia a clave criptográfica remota seleccionada, recibida procedente del sistema informático cliente, como la clave criptográfica remota a utilizar para la realización de la operación criptográfica.

3. Procedimiento según cualquiera de las reivindicaciones 1 o 2, que comprende además:
• obtener, por parte del sistema informático cliente, un conjunto de referencias a claves criptográficas locales permitidas para la petición de usuario de un repositorio de claves criptográficas locales comprendido en el sistema informático cliente;
• establecer, por parte del sistema informático cliente, una clave criptográfica local referenciada en el conjunto de referencias a claves criptográficas locales como la clave criptográfica local a utilizar para la realización de la operación criptográfica;
• realizar, por parte del sistema informático cliente, la operación criptográfica usando la clave criptográfica local a utilizar para la realización de la operación criptográfica.

4. Procedimiento según la reivindicación 3, que comprende además:
• seleccionar, por parte del sistema informático cliente, una referencia del conjunto de referencias a claves criptográficas locales según una petición de usuario para la selección de claves criptográficas locales;
y en el que establecer, por parte del sistema informático cliente, una clave criptográfica local referenciada en el conjunto de referencias a claves criptográficas locales como la clave criptográfica local a utilizar para la realización de la operación criptográfica comprende:
• establecer, por parte del sistema informático cliente, la clave criptográfica local referenciada por la referencia a clave criptográfica local seleccionada como la clave criptográfica local a utilizar para la realización de la operación criptográfica.

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que una clave criptográfica remota está permitida para la petición de usuario cuando dicha clave criptográfica remota y la petición de usuario se corresponden con una regla de contexto de uso de un conjunto de reglas de contexto de uso, y dicha regla de contexto de uso correspondida comprende una acción resultante que indica que está permitido el uso de la clave criptográfica remota.

6. Procedimiento según la reivindicación 5, en el que cada regla de contexto de uso del conjunto de reglas de contexto de uso comprende además una prioridad, y en el que una clave criptográfica remota está permitida para la petición de usuario cuando dicha clave criptográfica remota y la petición de usuario se corresponden con al menos

una regla de contexto de uso y la regla de contexto de uso de dicha al menos una regla de contexto de uso que tiene la prioridad más alta comprende una acción resultante que indica que está permitido el uso de la clave criptográfica remota.

7. Procedimiento según cualquiera de las reivindicaciones 5 o 6, en el que cada regla de contexto de uso comprende además un perfil de usuario y un perfil de clave criptográfica, y en el que una clave criptográfica remota y la petición de usuario se corresponden con una regla de contexto de uso cuando el usuario de la petición de usuario pertenece al perfil de usuario de dicha regla de contexto de uso y dicha clave criptográfica remota pertenece al perfil de clave criptográfica de dicha regla de contexto de uso.

8. Procedimiento según la reivindicación 7, en el que cada regla de contexto de uso comprende además un perfil de condiciones técnicas, y en el que una clave criptográfica remota y la petición de usuario se corresponden con una regla de contexto de uso cuando el usuario de la petición de usuario pertenece al perfil de usuario de dicha regla de contexto de uso, dicha clave criptográfica remota pertenece al perfil de clave criptográfica de dicha regla de contexto de uso, y las condiciones técnicas bajo las cuales se ha realizado la petición de usuario pertenecen al perfil de condiciones técnicas de dicha regla de contexto de uso.

9. Procedimiento según la reivindicación 8, en el que el perfil de condiciones técnicas se refiere a al menos uno de los siguientes parámetros: hora de la petición de usuario, perfil del sistema informático cliente, ubicación del sistema informático cliente, y perfil de la aplicación a través de la cual se ha realizado la petición de usuario.

10. Procedimiento según cualquiera de las reivindicaciones 1 a 9, que comprende además:
• almacenar, por parte del gestor de múltiples repositorios, datos relacionados con cada resultado de la operación criptográfica en un repositorio de eventos criptográficos.

11. Procedimiento según cualquiera de las reivindicaciones 1 a 10, que comprende además:
• almacenar, por parte del gestor de múltiples repositorios, datos relacionados con la petición de usuario recibida en el repositorio de eventos criptográficos.

12. Procedimiento de obtención de un resultado de una operación criptográfica en un sistema informático cliente, que comprende:
• enviar, por parte del sistema informático cliente, una petición de usuario de la operación criptográfica a un sistema informático servidor que comprende un gestor de múltiples repositorios y al menos un repositorio de claves criptográficas remotas;
• recibir, por parte del sistema informático cliente, el resultado de la operación criptográfica procedente del sistema informático servidor, siendo dicho resultado recibido de la operación criptográfica el resultado de:
• obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas;
• establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica;
• solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota;
• obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica.

13. Procedimiento según la reivindicación 12, que comprende además:
• recibir, por parte del sistema informático cliente, procedente del sistema informático servidor el conjunto de referencias a claves criptográficas remotas obtenido por el gestor de múltiples repositorios;
• seleccionar, por parte del sistema informático cliente, una referencia del conjunto de referencias a claves criptográficas remotas según una petición de usuario para la selección de claves criptográficas remotas;
• enviar, por parte del sistema informático cliente, la referencia a clave criptográfica remota seleccionada al sistema informático servidor para que el sistema informático servidor reciba dicha referencia a clave criptográfica remota, la cual ha sido seleccionada por el sistema informático cliente del conjunto de referencias a claves criptográficas remotas, y para que el gestor de múltiples repositorios establezca la clave criptográfica remota referenciada por dicha referencia a clave criptográfica remota seleccionada recibida como la clave criptográfica remota a utilizar para la realización de la operación criptográfica.

14. Producto de programa informático que comprende instrucciones de programa para hacer que un ordenador realice un procedimiento de obtención de un resultado de una operación criptográfica en un sistema informático cliente, dicho procedimiento según cualquiera de las reivindicaciones 12 o 13.

15. Producto de programa informático según la reivindicación 14, incluido en un medio de almacenamiento.

16. Producto de programa informático según la reivindicación 14, portado por una señal portadora.

17. Procedimiento de proporcionar un resultado de una operación criptográfica desde un sistema informático servidor, que comprende:
• recibir, por parte del sistema informático servidor, que comprende un gestor de múltiples repositorios y al menos un repositorio de claves criptográficas remotas, una petición de usuario de la operación criptográfica procedente de un sistema informático cliente;
• obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas;
• establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica;
• solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota;
• obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica;
• enviar, por parte del sistema informático servidor, el resultado de la operación criptográfica al sistema informático cliente.

18. Procedimiento según la reivindicación 17, que comprende además:
• enviar, por parte del sistema informático servidor, el conjunto obtenido de referencias a claves criptográficas remotas al sistema informático cliente;
y en el que establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica comprende:
• establecer, por parte del gestor de múltiples repositorios, la clave criptográfica remota referenciada por una referencia a clave criptográfica remota seleccionada, recibida procedente del sistema informático cliente, como la clave criptográfica remota a utilizar para la realización de la operación criptográfica; en el que la referencia a clave criptográfica remota seleccionada es el resultado de:
• seleccionar, por parte del sistema informático cliente, una referencia del conjunto de referencias a claves criptográficas remotas, recibidas procedentes del sistema informático servidor, según una petición de usuario para la selección de claves criptográficas remotas.

19. Un producto de programa informático que comprende instrucciones de programa para hacer que un ordenador realice un procedimiento para proporcionar un resultado de una operación criptográfica desde un sistema informático servidor, dicho procedimiento según cualquiera de las reivindicaciones 17 o 18.

20. Sistema para realizar una operación criptográfica, que comprende al menos un sistema informático cliente y un sistema informático servidor; en el que el sistema informático servidor comprende un gestor de múltiples repositorios, al menos un repositorio de claves criptográficas remotas, un procesador y una memoria; en el que el sistema informático cliente comprende un procesador y una memoria; y en el que la memoria del sistema informático servidor y la memoria del sistema informático cliente almacenan instrucciones ejecutables por ordenador que, cuando son ejecutadas, hacen que los sistemas informáticos cliente y servidor realicen un procedimiento que comprende:
• enviar, por parte del sistema informático cliente, una petición de usuario de la operación criptográfica al sistema informático servidor;
• obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas;
• establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica;
• solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota;
• obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica;
• enviar, por parte del sistema informático servidor, el resultado de la operación criptográfica al sistema informático cliente.

21. Sistema informático cliente para obtener un resultado de una operación criptográfica en el sistema informático cliente, comprendiendo el sistema informático cliente un procesador y una memoria; en el que la memoria del sistema informático cliente almacena instrucciones ejecutables por ordenador que, cuando son ejecutadas, hacen que el sistema informático cliente realice un procedimiento que comprende:
• enviar, por parte del sistema informático cliente, una petición de usuario de la operación criptográfica a un sistema informático servidor que comprende un gestor de múltiples repositorios y al menos un repositorio de claves criptográficas remotas;
• recibir, por parte del sistema informático cliente, el resultado de la operación criptográfica procedente del sistema informático servidor, siendo dicho resultado recibido de la operación criptográfica el resultado de:
• obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas;
• establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica;
• solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota;
• obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica.

22. Sistema informático servidor para proporcionar un resultado de una operación criptográfica, comprendiendo el sistema informático servidor un gestor de múltiples repositorios, al menos un repositorio de claves criptográficas remotas, un procesador y una memoria; en el que la memoria del sistema informático servidor almacena instrucciones ejecutables por ordenador que, cuando son ejecutadas, hacen que el sistema informático servidor realice un procedimiento que comprende:
• recibir, por parte del sistema informático servidor, una petición de usuario de la operación criptográfica procedente de un sistema informático cliente;
• obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas;
• establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica;
• solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota;
• obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica;
• enviar, por parte del sistema informático servidor, el resultado de la operación criptográfica al sistema informático cliente.

23. Sistema para realizar una operación criptográfica, que comprende al menos un sistema informático cliente que comprende:
• medios informáticos para enviar una petición de usuario de la operación criptográfica al sistema informático servidor;
• medios informáticos para recibir el resultado de la operación criptográfica procedente del sistema informático servidor;
y un sistema informático servidor que comprende:
• medios informáticos para recibir la petición de usuario de la operación criptográfica procedente del sistema informático cliente;
• medios informáticos para enviar el resultado de la operación criptográfica al sistema informático cliente;
• al menos un repositorio de claves criptográficas remotas; y
• un gestor de múltiples repositorios que comprende:
• medios informáticos para obtener un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas;
• medios informáticos para establecer una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica;
• medios informáticos para solicitar la ejecución de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota;
• medios informáticos para obtener el resultado de la operación criptográfica procedente del repositorio de claves

criptográficas remotas que ha realizado la operación criptográfica.

24. Sistema informático cliente para obtener un resultado de una operación criptográfica en el sistema informático cliente, que comprende:
• medios informáticos para enviar una petición de usuario de la operación criptográfica a un sistema informático servidor que comprende un gestor de múltiples repositorios y al menos un repositorio de claves criptográficas remotas;
• medios informáticos para recibir el resultado de la operación criptográfica procedente del sistema informático servidor, siendo dicho resultado recibido de la operación criptográfica el resultado de:
• obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas;
• establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica;
• solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota;
• obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica.

25. Sistema informático servidor para proporcionar un resultado de una operación criptográfica, que comprende:
• medios informáticos para recibir una petición de usuario de la operación criptográfica procedente de un sistema informático cliente;
• medios informáticos para enviar el resultado de la operación criptográfica al sistema informático cliente;
• al menos un repositorio de claves criptográficas remotas; y
• un gestor de múltiples repositorios que comprende:
• medios informáticos para obtener un conjunto de referencias a claves criptográficas remotas permitidas para la petición de usuario del al menos un repositorio de claves criptográficas remotas;
• medios informáticos para establecer una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica;
• medios informáticos para solicitar la ejecución de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota;
• medios informáticos para obtener el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica.

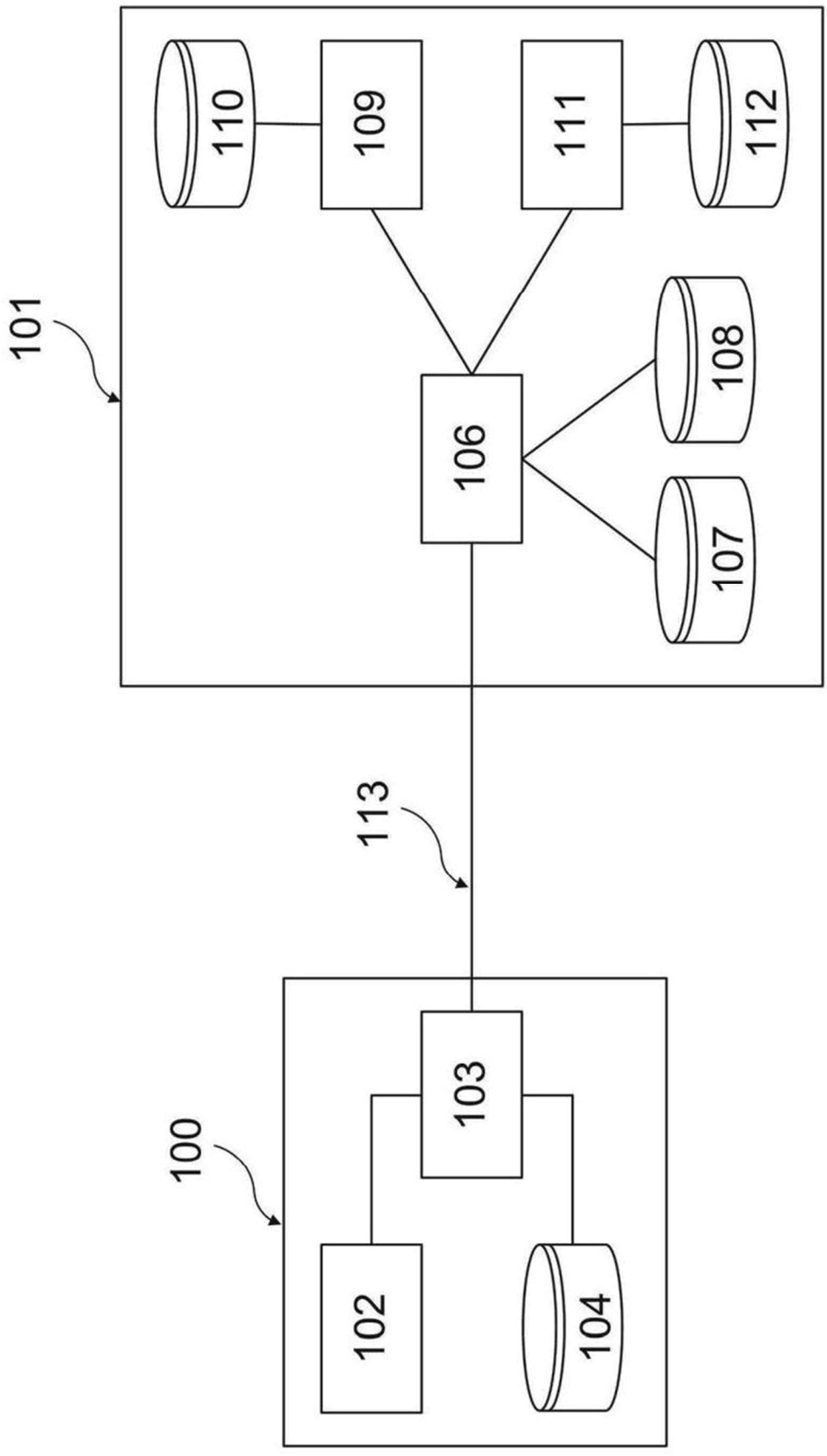

FIG.1

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201490042

(22) Fecha de presentación de la solicitud: 13.10.2011

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L9/08*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	EP 1755269 A1 (NEC CORP) 21.02.2007, resumen; párrafos 49,66-71; reivindicaciones 1,6-7,10,15,18.	1-25
A	WO 0065766 A2 (DISAPPEARING INC et al.) 02.11.2000, todo el documento.	1
A	US 2006062392 A1 (LEE KEUN M et al.) 23.03.2006, todo el documento.	1
A	US 2002071560 A1 (KURN DAVID MICHAEL et al.) 13.06.2002, todo el documento.	1
A	US 2005071632 A1 (PAUKER MATTHEW J et al.) 31.03.2005, todo el documento.	1

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
01.04.2015	M. Muñoz Sánchez	1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 01.04.2015

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	2-11, 13, 15-16, 18	**SI**
	Reivindicaciones	1, 12, 14, 17, 19-25	**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	2-11, 13, 15-16, 18	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	EP 1755269 A1 (NEC CORP)	21.02.2007
D02	WO 0065766 A2 (DISAPPEARING INC et al.)	02.11.2000
D03	US 2006062392 A1 (LEE KEUN M et al.)	23.03.2006
D04	US 2002071560 A1 (KURN DAVID MICHAEL et al.)	13.06.2002
D05	US 2005071632 A1 (PAUKER MATTHEW J et al.)	31.03.2005

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento más próximo del estado de la técnica al objeto de la solicitud.

Reivindicaciones independientes

Reivindicación 1: El documento D01 divulga un método que comprende:
 enviar por parte de un sistema informático cliente una petición de usuario de la operación criptográfica a un sistema informático servidor que comprende un gestor de múltiples repositorios y al menos un repositorio de claves criptográficas remotas; (resumen, pár. 49)

- obtener, por parte del gestor de múltiples repositorios, un conjunto de referencias a claves criptográficas remotas (pár. 66-71)
- establecer, por parte del gestor de múltiples repositorios, una clave criptográfica remota referenciada en el conjunto de referencias a claves criptográficas remotas como la clave criptográfica remota a utilizar para la realización de la operación criptográfica; (pár. 66-71)
- solicitar, por parte del gestor de múltiples repositorios, la realización de la operación criptográfica al repositorio en el que está almacenada la clave criptográfica remota a utilizar, para que dicha operación criptográfica sea realizada usando dicha clave criptográfica remota; (pár. 66-71)
- obtener, por parte del gestor de múltiples repositorios, el resultado de la operación criptográfica procedente del repositorio de claves criptográficas remotas que ha realizado la operación criptográfica; (pár. 66-71)
- enviar, por parte del sistema informático servidor, el resultado de la operación criptográfica al sistema informático cliente (pár. 67)

El documento D01 también divulga varias alternativas de selección de la clave criptográfica a utilizar en función del nivel de seguridad necesario, existiendo un repositorio para cada nivel de seguridad.
El documento D01 divulga así todas las características técnicas de la reivindicación 1 y por tanto afecta a la novedad de dicha reivindicación 1 según el art. 6.1 de la Ley 11/86 de Patentes.

Reivindicaciones 12, 14, 17, 19 y 20-25: las reivindicaciones de método, productos de programa de ordenador y sistemas se corresponden directamente con las del método de la reivindicación 1 y, por tanto, se encuentran implícitamente también en el documento D01. Así estas reivindicaciones carecen de novedad según el art. 6.1 de la Ley 11/86 de Patentes.

Reivindicaciones dependientes

Reivindicaciones 2-11: la utilización de reglas de contexto, perfiles u operaciones concretas, por ejemplo, para determinar el nivel de seguridad y con ello el grupo de referencias a claves criptográficas adecuado es una opción común en el campo técnico de la solicitud y por tanto evidente para el experto en la materia. Por la misma razón la utilización de preferencias del usuario a la hora de elegir una clave de entre varias para la realización de operaciones criptográficas también es evidente para el experto en la materia. La realización de estas operaciones remota o localmente en función de un nivel de seguridad concreto también es una opción común y así evidente para el experto en la materia. Por último el registro de eventos no contribuye al método de selección de claves criptográficas en sí y el hecho de que se haga sólo tiene un carácter meramente informativo (resultado correcto/ incorrecto, número de petición de usuario etc.). Estas posibilidades se pueden ver en los documentos D02, D03, D04 o D05.
Por tanto, el documento D01 también afecta a la actividad inventiva de las reivindicaciones 2-11 según el art. 8.1 de la Ley 11/86 de Patentes.

Reivindicaciones 13, 15-16 y 18: estas reivindicaciones tratan las mismas características técnicas y de la misma manera que las reivindicaciones 2-11 analizadas antes por lo que su evaluación coincide con las de dichas reivindicaciones 2-11. En conclusión, el documento D01 también afecta a la actividad inventiva de las reivindicaciones 13, 15-16 y 18 según el art. 8.1 de la Ley 11/86 de Patentes.