(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 800 295**

(51) Int. CI.:

H04L 9/08 (2006.01)
G06F 21/62 (2013.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.02.2017 PCT/GB2017/050264**

(87) Fecha y número de publicación internacional: **10.08.2017 WO17134445**

(96) Fecha de presentación y número de la solicitud europea: **03.02.2017 E 17704057 (3)**

(97) Fecha y número de publicación de la concesión europea: **25.03.2020 EP 3412001**

(54) Título: **Método de transferencia de datos y dispositivos criptográficos**

(30) Prioridad:

05.02.2016 GB 201602088

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.12.2020

(73) Titular/es:

NCIPHER SECURITY LIMITED (100.0%)
1 Station Square
Cambridge CB1 2GA, GB

(72) Inventor/es:

BYGRAVE, IAN;
EDGINGTON, ALEC;
KETTLEWELL, RICHARD;
O'DOHERTY, DAVID;
SMITH, NICHOLAS y
WALKER, NEIL

(74) Agente/Representante:

FLORES DREOSTI, Lucas

DESCRIPCIÓN

Método de transferencia de datos y dispositivos criptográficos

Campo

[0001] La presente invención hace referencia a métodos de transferencia de datos, métodos de control del uso de datos y dispositivos criptográficos.

Antecedentes

[0002] Internet ha dado lugar a que numerosas organizaciones utilicen servicios implementados por ordenador alojados por un proveedor de servicios que anteriormente habrían tenido que alojar ellas mismas. Los proveedores de servicios son capaces de proporcionar servicios implementados por ordenador a un gran número de organizaciones (inquilinos o *tenants*). Un ejemplo de esto son los proveedores de servicios en la nube, CSP por sus siglas en inglés, quienes ofrecen productos como "*software* como servicio" (SaaS, por sus siglas en inglés) o almacenamiento bajo demanda. El uso de un servicio implementado por ordenador alojado por un proveedor de servicios permite que los inquilinos reduzcan los gastos de administración de alojar tales servicios ellos mismos.

[0003] Un área en la que los proveedores de servicios se han esforzado por ofrecer un servicio implementado por ordenador multitenencia es en el sector de infraestructura criptográfica, y específicamente en módulos de seguridad de hardware, HSM.

[0004] Un HSM convencional alojado por un proveedor de servicios utiliza una solución para un solo inquilino (*single-tenancy*), es decir, un dispositivo dedicado por inquilino, para permitir el procesamiento criptográfico de datos y almacenamiento de claves criptográficas seguro en nombre del inquilino. El proveedor de servicios gestiona los ajustes de entorno del dispositivo criptográfico, como la dirección IP, mientras que el inquilino gestiona la infraestructura criptográfica de manera remota de forma convencional. De este modo, el proveedor de servicios tiene que facilitar un dispositivo por inquilino, mientras que el inquilino tiene que gestionar el mantenimiento y administración del dispositivo criptográfico como lo habría hecho previamente. Dicho sistema es ineficiente y a menudo resulta en la infrautilización de recursos criptográficos.

[0005] Además, dicho sistema puede ser vulnerable. El proveedor de servicios a menudo tiene las "llaves del reino", es decir, la capacidad de exportar el material de claves bruto almacenado en el HSM. Los permisos otorgados al proveedor de servicios pueden menoscabar la seguridad de una clave de inquilino alojada. Esto da lugar a una variedad de problemas tanto para el inquilino como para el proveedor de servicios, incluyendo el posible uso fraudulento de una clave criptográfica del inquilino por el proveedor de servicios, la exposición de una clave del inquilino a una agencia de seguridad que tiene jurisdicción sobre el proveedor de servicios, pero no el inquilino, y el uso de una clave del inquilino por otro inquilino.

[0006] US 2014/229739 describe un sistema que utiliza información enviada en relación con una solicitud para determinar si procesa la solicitud y cómo lo hace.

[0007] "Data Sheet: Vormetric Data Security Platform" (https://www.vormetric.com/sites/default/files/ds-vormetric-datasecurity-platform-web-0622.pdf) describe una plataforma de seguridad de datos que ofrece capacidades para el cifrado a nivel de archivo transparente, cifrado de capa de aplicación, tokenización, enmascaramiento de datos dinámico, *cloud encryption gateway*, gestión de claves integrada, control de acceso de usuarios privilegiados e inteligencia de seguridad.

[0008] "White Paper Vormetric Data Security Platform Architecture" (http://enterprise-encryption.vormetric.com/rs/480-LWA-970/images/ Vormetric_Data_Security_Platform_Architecture_WhitePaper.pdf) describe un resumen de los diferentes métodos de cifrado disponibles.

[0009] WO 2015/012933 describe un método de gestión de claves y políticas.

[0010] US 2003/0021417 describe un sistema informático que contiene claves criptográficas e indentificadores de claves criptográficas.

[0011] Robert Griffin ET AL: "PKCS #11 Cryptographic Token Interface Base Specification Version 2.40" (http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.html) define tipos de datos, funciones y otros componentes básicos del interfaz PKCS#11 Cryptoki.

[0012] US 2014/0230007 describe que la solicitud enviada a un sistema informático es evaluada para el cumplimiento de la política que garantiza la seguridad de los datos.

[0013] "Vormetric Encryption of VMware Customer Data at Rest @ SoftLayer", (http://wpc.c320.edgecastcdn.net/O0C320/VMware@Softlayer Vormetric Encryption draft vl 2.pdf) describe cómo los datos en reposo son cifrados en una infraestructura VMware prestada en la nube de Softlayer.

[0014] "Vormetric Encryption Expert Cryptographic Module Software Version 4.4.1 FIPS 140-2 Non- Proprietary Security Policy Level 1 Validation" (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1721.pdf) describe cómo este módulo cumple todos los requisitos especificados en los requisitos FIPS 140-2 Nivel 1.

[0015] US 2014/143543 describe en un servicio de almacenamiento alojado, un recurso y se recibe una solicitud para almacenar el recurso, donde la solicitud incluye una localización de un servicio de control de acceso.

Declaraciones de la Invención

[0016] La invención se expone en las reivindicaciones independientes.

[0017] En un primer aspecto de la presente invención, se proporciona un método de transferencia de datos entre un primer contexto de seguridad en un sistema de inquilino y un segundo contexto de seguridad en un sistema de proveedor de servicios, comprendiendo el método:

generar una lista de control de acceso correspondiente a los datos en el primer contexto de seguridad, donde la lista de control de acceso especifica que debe presentarse credencial de uso válida para permitir un primer tipo de uso de los datos;

generar un primer par de claves criptográficas y un primer certificado criptográfico en el segundo contexto de seguridad, comprendiendo el primer par de claves criptográficas una primera clave pública, $K_{BLOB\ pub}$, y una primera clave privada, $K_{BLOB\ priv}$ y el primer certificado criptográfico comprendiendo información a partir de la cual el origen de la primera clave pública $K_{BLOB\ pub}$ puede ser validado;

enviar la primera clave pública $K_{BLOB\ pub}$ y el primer certificado criptográfico al primer contexto de seguridad;

validar el primer certificado criptográfico en el primer contexto de seguridad;

si el primer certificado criptográfico es válido, cifrar los datos y la lista de control de acceso correspondiente con la primera clave pública $K_{BLOB\ pub}$ en el primer contexto de seguridad;

enviar los datos y lista de control de acceso correspondiente cifrados, e información a partir de la cual el origen de los datos puede validarse, al segundo contexto de seguridad.

[0018] En un modo de realización, la credencial de uso es un certificado de uso.

[0019] En un modo de realización, los datos comprenden una clave criptográfica, K_{tenant}. El método puede comprender además la etapa de generar la clave criptográfica, K_{tenant} en el primer contexto de seguridad. El primer tipo de uso puede ser una o más operaciones criptográficas.

[0020] En un modo de realización, el método comprende además establecer en el sistema de inquilino que el segundo contexto de seguridad es de confianza, antes de enviar los datos cifrados.

[0021] Establecer la confianza puede comprender validar en el primer contexto de seguridad que el segundo contexto de seguridad es fabricado por un fabricante de confianza, que la configuración del segundo contexto de

seguridad cumple los requisitos de seguridad del inquilino y que el segundo contexto de seguridad está configurado para aplicar las políticas contenidas en la ACL.

[0022] En un modo de realización, se valida que la configuración del segundo contexto de seguridad cumple los requisitos de seguridad del inquilino inmediatamente antes de la transferencia de los datos cifrados al segundo contexto de seguridad.

[0023] Establecer confianza puede comprender además validar que el estado del segundo contexto de seguridad cumple con los requisitos de seguridad del fabricante, por ejemplo, validando que el *software* y *hardware* son impermeables a ataques del proveedor de servicios.

[0024] Puede usarse una clave privada de fabricante para validad que el segundo contexto de seguridad es fabricado por un fabricante de confianza, y para validar una segunda clave pública de identidad del segundo contexto de seguridad.

[0025] En un modo de realización, el segundo contexto de seguridad almacena una segunda clave privada de identidad, $K_{2ID\ priv}$, y el método comprende además enviar la segunda clave pública de identidad, $K_{2ID\ pub}$, y un segundo certificado de identidad desde el segundo contexto de seguridad al primer contexto de seguridad, donde la segunda clave pública de identidad, $K_{2ID\ pub}$ y la segunda clave privada de identidad, $K_{2ID\ priv}$ son un par de claves criptográficas y el segundo certificado de identidad comprende información que identifica a $K_{2ID\ pub}$ y está firmada de manera criptográfica por la clave privada de fabricante $K_{man\ priv}$.

[0026] En un modo de realización, el segundo certificado de identidad comprende además información a partir de la cual puede validarse el estado del segundo contexto de seguridad.

[0027] En un modo de realización, el método comprende además establecer en el sistema de inquilino que una fuente de tiempo de referencia es de confianza. En un modo de realización, el método comprende además establecer en el sistema de proveedor de servicio que una fuente de tiempo de referencia es de confianza. Establecer que una fuente de tiempo de referencia es de confianza comprende validar que la fuente de tiempo de referencia es fabricada por un fabricante de confianza y que el estado y configuración de la fuente de tiempo de referencia cumple los requisitos de seguridad.

[0028] En un modo de realización, el método comprende además:

generar información relativa a la configuración actual del segundo contexto de seguridad;
firmar criptográficamente la información con la segunda clave privada de identidad, $K_{2ID\ priv}$;
enviar la información firmada desde el segundo contexto de seguridad al primer contexto de seguridad.

[0029] En un modo de realización, el primer certificado criptográfico comprende la información relativa a la configuración actual del segundo contexto de seguridad y es firmado con la segunda clave privada de identidad, $K_{2ID\ priv}$.

[0030] En un modo de realización, el método comprende además:

generar un segundo par de claves criptográficas y un segundo certificado criptográfico en el primer contexto de seguridad, comprendiendo el segundo par de claves criptográficas una segunda clave pública, $K_{tenant\text{-}signpub}$, y una segunda clave privada, $K_{tenant\text{-}signpriv}$ y el segundo certificado criptográfico comprendiendo información a partir de la cual el origen de la segunda clave pública $K_{tenant\text{-}signpub}$ puede ser validado;
enviar la segunda clave pública $K_{tenant\text{-}signpub}$ y el segundo certificado criptográfico al segundo contexto de seguridad.

[0031] En un modo de realización, el primer contexto de seguridad almacena una primera clave privada de identidad, $K_{1ID\ priv}$, y el método comprende además:

enviar una primera clave pública de identidad, $K_{1ID\ pub}$, y un primer certificado de identidad desde el primer contexto de seguridad al segundo contexto de seguridad, donde la primera clave pública de identidad, $K_{11D\ pub}$ y la primera clave privada de identidad, $K_{1ID\ priv}$ son un par de claves criptográficas y el primer certificado de identidad comprende información que identifica $K_{1ID\ pub}$ y es firmado de manera criptográfica por una clave privada de fabricante $K_{man\ priv}$.

[0032] En un modo de realización, el segundo certificado criptográfico comprende información a partir de la cual el origen de la segunda clave pública $K_{tenant\text{-}signpub}$ puede ser identificado; y el método comprende además:

firmar criptográficamente el segundo certificado criptográfico con la primera clave privada de identidad, $K_{1ID\ priv}$;

verificar el segundo certificado criptográfico utilizando la primera clave pública de identidad, $K_{1ID\ pub}$ en el segundo contexto de seguridad.

[0033] La información a partir de la cual el origen de la clave criptográfica K_{tenant} puede validarse puede comprender la clave criptográfica K_{tenant} y la lista de control de acceso correspondiente cifradas firmadas con $K_{tenant\text{-}signpriv}$.

[0034] El paso de enviar la clave criptográfica K_{tenant} y lista de control de acceso correspondiente cifradas, e información a partir de la cual el origen de la clave criptográfica K_{tenant} puede validarse, al segundo contexto de seguridad (7) puede comprender:

firmar criptográficamente la clave criptográfica K_{tenant} y la lista de control de acceso correspondiente cifradas con $K_{tenant\text{-}signpriv}$;

enviar la clave criptográfica K_{tenant} y lista de control de acceso correspondiente cifradas, la firma de la clave criptográfica K_{tenant} y lista de control de acceso correspondiente cifradas y el *hash* de $K_{tenant\text{-}signpub}$ al segundo contexto de seguridad.

[0035] En un modo de realización, el primer certificado criptográfico valida que $K_{BLOB\ priv}$ es efímero y que $K_{BLOB\ priv}$ no puede salir del segundo contexto de seguridad. En un modo de realización, el primer certificado criptográfico valida que el par de claves asimétricas fue generado en el segundo contexto de seguridad. La primera clave privada, $K_{BLOB\ priv}$ es almacenada en el segundo contexto de seguridad.

[0036] En un modo de realización, la información a partir de la cual puede validarse el origen de la primera clave pública $K_{BLOB\ pub}$ es un *hash* firmado de la primera clave pública, $K_{BLOB\ pub}$. El primer certificado criptográfico comprende un *hash* de la primera clave pública, $K_{BLOB\ pub}$ y es firmado con la mitad privada de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ priv}$. El paso de validar el primer certificado criptográfico, C_{BLOB}, comprende verificar la firma utilizando la mitad pública de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ pub}$.

[0037] En un modo de realización, el segundo contexto de seguridad está protegido del resto del sistema de proveedor de servicios.

[0038] En un modo de realización, la lista de control de acceso (ACL, por sus siglas en inglés) especifica que la credencial de uso debe comprender información a partir de la cual el origen de la credencial de uso puede ser validado. La lista de control de acceso puede especificar que la credencial de uso es un certificado de uso que debe ser firmado por la segunda clave privada $K_{tenant\text{-}signpriv}$ para permitir el primer tipo de uso de la clave criptográfica, K_{tenant}.

[0039] La ACL especifica que la credencial de uso debe comprender información a partir de la cual pueda determinarse la expiración de la credencial de uso y no debe haber expirado para ser válida.

[0040] La ACL puede especificar que la clave criptográfica de inquilino K_{tenant} puede ser almacenada exclusivamente en la memoria no volátil que sea resistente a manipulaciones por terceros.

[0041] En un modo de realización, la ACL especifica que la clave criptográfica de inquilino K_{tenant} puede almacenarse exclusivamente dentro del segundo contexto de seguridad. En un modo de realización alternativo, la ACL contiene una restricción de que la clave criptográfica de inquilino K_{tenant} puede ser almacenada exclusivamente con la condición de que sea cifrada para su almacenamiento mediante un clave que no puede salir del segundo contexto de seguridad.

[0042] En un modo de realización, el método comprende además:

validar, en el segundo contexto de seguridad, el origen de la clave criptográfica K_{tenant};

descifrar la clave criptográfica K_{tenant} y la lista de control de acceso correspondiente cifradas con la primera clave privada $K_{BLOB\ priv}$ en el segundo contexto de seguridad.

[0043] En un modo de realización, el método comprende además:

recifrar la clave criptográfica K_{tenant} con una clave criptográfica adicional en el segundo contexto de seguridad, donde la clave criptográfica adicional no puede dejar el segundo contexto de seguridad;

almacenar la clave criptográfica recifrada K_{tenant}, lista de control de acceso correspondiente, e información a partir de la cual el orginen de la clave criptográfica K_{tenant} puede validarse.

[0044] En un aspecto adicional de la presente invención, se proporciona un medio portador que comprende un código legible por ordenador configurado para hacer que un ordenador lleve a cabo cualquiera de los métodos descritos.

[0045] En otro aspecto de la presente invención, se proporciona un método de control de uso de datos, siendo almacenados los datos en un sistema de proveedor de servicios de manera que son accesibles para un segundo contexto de seguridad de confianza en el sistema de proveedor de servicios, pero están protegidos frente al resto del sistema de proveedor de servicios, donde la lista de control de acceso que especifica que una credencial de uso válida debe presentarse para permitir un primer tipo de uso de los datos es almacenada con los datos, comprendiendo el método:

generar una credencial de uso en un primer contexto de seguridad, donde la credencial de uso comprende:

información a partir de la cual los datos que corresponden a la credencial de uso pueden ser identificados;

información a partir de la cual la expiración de la credencial de uso puede ser determinada;

emitir la credencial de uso e información a partir de la cual el origen de la credencial de uso puede ser validado;

validar la credencial de uso con respecto a la lista de control de acceso, y validar que la credencial de uso no ha expirado en el segundo contexto de seguridad;

permitir el primer tipo de uso de los datos, en el segundo contexto de seguridad, con la condición de que la credencial de uso sea válida y no haya expirado.

[0046] En un modo de realización, la credencial de uso es un certificado de uso.

[0047] En un modo de realización, los datos comprenden una clave criptográfica, K_{tenant}. El primer tipo de uso puede ser una o más operaciones criptográficas.

[0048] En un modo de realización, la información a partir de la cual la expiración de la credencial de uso puede determinarse comprende:

un tiempo de expiración;

información que identifica una fuente de tiempo de referencia.

[0049] En un modo de realización, el método comprende además establecer en el sistema de inquilino que una fuente de tiempo de referencia es de confianza. En un modo de realización, el método comprende además

establecer en el sistema de proveedor de servicios que una fuente de tiempo de referencia de confianza. Establecer que una fuente de tiempo de referencia es de confianza comprende validar que la fuente de tiempo de referencia es fabricada por un fabricante de confianza y que el estado y configuración de la fuente de tiempo de referencia cumple los requisitos de seguridad.

[0050] En un modo de realización, el método comprende además proporcionar la mitad pública de un par de claves criptográficas de identidad de la fuente de tiempo al primer contexto de seguridad, junto con información que valide el origen del par de claves criptográficas de identidad.

[0051] En un modo de realización, el método comprende además proporcionar la mitad pública de un par de claves criptográficas de identidad de la fuente de tiempo al segundo contexto de seguridad, junto con información que valide el origen del par de claves criptográficas de identidad.

[0052] En un modo de realización, generar una credencial de uso en un primer contexto de seguridad comprende:

seleccionar una fuente de tiempo de referencia;
solicitar el sello de tiempo actual de la fuente de tiempo de referencia
calcular el tiempo de expiración basado en el sello de tiempo.

[0053] En un modo de realización, el método comprende:

enviar un mensaje que comprende el sello de tiempo actual de la fuente de tiempo de referencia al sistema de inquilino, junto con información a partir de la cual puede validarse el origen del mensaje; y
validar el origen del mensaje.

[0054] El mensaje puede comprender además información relativa a la configuración actual de la fuente de tiempo de referencia.

[0055] La información que valida el origen del mensaje puede ser el mensaje firmado, firmado con la mitad privada del par de claves criptográficas de identidad de la fuente de tiempo.

[0056] En un modo de realización, la información relativa a un tiempo de inicio se incluye en la credencial de uso.

[0057] La información a partir de la cual los datos que corresponden a la credencial de uso pueden ser identificados puede ser un *hash* de K_{tenant}.

[0058] En un modo de realización, la credencial de uso es un certificado de uso y el método comprende además:

firmar de manera criptográfica el certificado de uso con una clave privada $K_{tenant\text{-}signpriv}$ en el primer contexto de seguridad, donde la información a partir de la cual puede validarse el origen del certificado de uso es la firma y donde la integridad de la clave pública correspondiente $K_{tenant\text{-}signpub}$ es protegida y dicha clave es accesible al segundo contexto de seguridad;
verificar el certificado de uso utilizando la clave pública $K_{tenant\text{-}signpub}$ en el segundo contexto de seguridad.

[0059] En un modo de realización, el método comprende además:

proporcionar la credencial de uso, la información a partir de la cual puede validarse el origen de la credencial de uso, y una solicitud para llevar a cabo una operación con la clave K_{tenant}, siendo la operación un primer tipo de uso, al segundo contexto de seguridad;
llevar a cabo la operación en el segundo contexto de seguridad, con la condición de que la credencial de uso sea válida y no haya expirado.

[0060] En un modo de realización, validar que la credencial de uso no ha expirado en el segundo contexto de seguridad comprende:

solicitar el sello de tiempo actual de la fuente de tiempo de referencia;

enviar un mensaje que comprende el sello de tiempo actual de la fuente de tiempo de referencia al segundo contexto de seguridad, junto con información a partir de la cual puede validarse el origen del mensaje; y

validar el origen del mensaje.

[0061] La información que valida el origen del mensaje puede ser el mensaje firmado, firmado con la mitad privada del par de claves criptográficas de identidad de la fuente de tiempo.

[0062] Validar que la credencial de uso no ha expirado en el segundo contexto de seguridad puede comprender además:

comparar el sello de tiempo con el tiempo de expiración.

[0063] En un aspecto adicional de la presente invención, se proporciona un medio portador que comprende un código legible por ordenador configurado para hacer que un ordenador lleve a cabo cualquiera de los métodos descritos.

[0064] En un aspecto adicional de la presente invención, se proporciona un dispositivo criptográfico que comprende un primer contexto de seguridad, el primer contexto de seguridad comprendiendo:

un primer transceptor configurado para recibir una primera clave pública $K_{BLOB\ pub}$ y un primer certificado criptográfico, comprendiendo información a partir de la cual puede validarse el origen de la primera clave pública $K_{BLOB\ pub}$, de un segundo contexto de seguridad;

un primer procesador configurado para llevar a cabo operaciones criptográficas, el primer procesador estando configurado para:

generar una lista de control de acceso que corresponde a los datos a ser transferidos, donde la lista de control de acceso especifica que debe presentarse una credencial de uso válida para permitir un primer tipo de uso de los datos;

validar que el primer par de claves criptográficas se originó desde el segundo contexto de seguridad;

cifrar los datos y la lista de control de acceso correspondiente con la primera clave pública $K_{BLOB\ pub}$;

donde el primer transceptor está configurado para enviar los datos y lista de control de acceso correspondiente cifrados, e información a partir de la cual el origen de los datos puede validarse, al segundo contexto de seguridad.

[0065] En un modo de realización, la credencial de uso es un certificado de uso.

[0066] En un modo de realización, los datos comprenden una clave criptográfica, K_{tenant}.

[0067] En un modo de realización, el dispositivo comprende además:

una primera memoria de dispositivo, que almacena una primera clave privada de identidad, $K_{1ID\ priv}$;

donde el primer transceptor es configurado además para:

enviar una primera clave pública de identidad, $K_{1ID\ pub}$, y un primer certificado de identidad al segundo contexto de seguridad, donde la primera clave pública de identidad, $K_{1ID\ pub}$ y la primera clave privada de identidad, $K_{1ID\ priv}$ son un par de claves criptográficas y el primer certificado de identidad comprende información que identifica $K_{1ID\ pub}$ y es firmado de manera criptográfica por una clave privada de fabricante $K_{man\ priv}$; y

recibir una segunda clave pública de identidad, $K_{2ID\ pub}$, y un segundo certificado de identidad del segundo contexto de seguridad, el segundo certificado de identidad comprendiendo

información que identifica a $K_{2ID\ pub}$ y estando firmado criptográficamente por la clave privada de fabricante $K_{man\ priv}$;

el primer procesador está configurado además para verificar el segundo certificado de identidad utilizando la clave pública de fabricante $K_{man\ pub}$.

[0068] En un modo de realización, el primer transceptor está configurado además para:

recibir información relativa a la configuración actual del segundo contexto de seguridad, donde la información está firmada criptográficamente con una segunda clave privada de identidad, $K_{2ID\ priv}$, donde la segunda clave pública de identidad, $K_{2ID\ pub}$ y la segunda clave privada de identidad, $K_{2ID\ priv}$ son un par de claves criptográficas, y donde

el primer procesador está configurado además para:

verificar la firma utilizando la segunda clave pública de identidad, $K_{2ID\ pub}$;

validar que la configuración del segundo contexto de seguridad cumple los requisitos de seguridad del inquilino y que el segundo contexto de seguridad está configurado para aplicar las políticas contenidas en la ACL.

[0069] En un modo de realización, el primer procesador está configurado además para:

generar un segundo par de claves criptográficas y un segundo certificado criptográfico en el primer contexto de seguridad, comprendiendo el segundo par de claves criptográficas una segunda clave pública, $K_{tenant\text{-}signpub}$, y una segunda clave privada, $K_{tenant\text{-}singpriv}$ y el segundo certificado criptográfico comprendiendo información a partir de la cual el origen de la segunda clave pública $K_{tenant\text{-}signpub}$ puede ser identificado;

firmar criptográficamente el segundo certificado criptográfico con la primera clave privada de identidad, $K_{1ID\ priv}$;

donde el primer transceptor está configurado además para enviar la segunda clave pública $K_{tenant\text{-}signpub}$ y el segundo certificado criptográfico firmado al segundo contexto de seguridad.

[0070] En un aspecto adicional de la presente invención, se proporciona un dispositivo criptográfico que comprende un primer contexto de seguridad, comprendiendo:

un primer procesador, configurado para generar una credencial de uso que comprende:

información a partir de la cual los datos que corresponden a la credencial de uso pueden ser identificados;

información a partir de la cual la expiración de la credencial de uso puede ser determinada;

un primer transceptor, configurado para enviar la credencial de uso e información a partir de la cual el origen de la credencial de uso puede ser validado a un segundo contexto de seguridad;

[0071] En un modo de realización, la credencial de uso es una credencial de uso.

[0072] En un modo de realización, los datos comprenden una clave criptográfica, K_{tenant}.

[0073] En un modo de realización, el primer contexto de seguridad comprende además:

una primera memoria de dispositivo, que almacena una clave privada $K_{tenant\text{-}signpriv}$;

donde el primer procesador está configurado para firmar criptográficamente la credencial de uso con la clave privada $K_{tenant\text{-}signpriv}$.

[0074] En un modo de realización, la credencial de uso es un certificado de uso.

[0075] En un modo de realización, la información a partir de la cual la expiración de la credencial de uso puede determinarse comprende:

un tiempo de expiración;

información que identifique una fuente de tiempo de referencia.

[0076] En un modo de realización, la información a partir de la cual la clave criptográfica K_{tenant} que corresponde a la credencial de uso puede ser identificada es un *hash* de K_{tenant}.

[0077] En un aspecto adicional de la presente invención, se proporciona un dispositivo criptográfico que comprende un segundo contexto de seguridad, para la cooperación con un dispositivo o dispositivos que comprenden un primer contexto de seguridad, el dispositivo criptográfico comprendiendo:

un procesador, configurado para llevar a cabo operaciones criptográficas, el procesador estando configurado para:

generar un primer par de claves criptográficas y un primer certificado criptográfico, comprendiendo el primer par de claves criptográficas una primera clave pública, $K_{BLOB\ pub}$, y una primera clave privada, $K_{BLOB\ priv}$ y el primer certificado criptográfico comprendiendo información a partir de la cual el origen de la primera clave pública $K_{BLOB\ pub}$ puede ser validado;

un transceptor, configurado para:

enviar la primera clave pública $K_{BLOB\ pub}$ y el primer certificado criptográfico a un primer contexto de seguridad; y

recibir datos cifrados y una lista de control de acceso correspondiente, e información a partir de la cual el origen de los datos puede validarse desde el primer contexto de seguridad;

el procesador configurado además para:

validar el origen de los datos;

descifrar los datos y la lista de control de acceso correspondiente cifrados utilizando la primera clave privada $K_{BLOB\ priv}$.

[0078] En un modo de realización, la credencial de uso es un certificado de uso.

[0079] En un modo de realización, los datos comprenden una clave criptográfica, K_{tenant}.

[0080] En un modo de realización, el procesador está configurado además para:

recifrar la clave criptográfica K_{tenant} con una clave criptográfica adicional, donde la clave criptográfica adicional no puede dejar el segundo contexto de seguridad.

[0081] En un modo de realización, el dispositivo comprende además una memoria de dispositivo, que almacena una segunda clave privada de identidad, $K_{2ID\ priv}$ y donde el transceptor está configurado además para:

enviar una segunda clave pública de identidad, $K_{2ID\ pub}$, y un segundo certificado de identidad al primer contexto de seguridad, donde la segunda clave pública de identidad, $K_{2ID\ pub}$ y la segunda clave privada de identidad, $K_{2ID\ priv}$ son un par de claves criptográficas y el segundo certificado de identidad comprende información que identifica $K_{2ID\ pub}$ y está firmado de manera criptográfica por una clave privada de fabricante $K_{man\ priv}$; y

recibir una primera clave pública de identidad, $K_{1ID\ pub}$, y un primer certificado de identidad del primer contexto de seguridad, el primer certificado de identidad comprendiendo información que identifica $K_{1ID\ pub}$ y estando firmado criptográficamente por la clave privada de fabricante $K_{man\ priv}$

el procesador está configurado además para;

verificar el primer certificado de identidad utilizando la clave pública de fabricante $K_{man\ pub}$.

[0082] En un modo de realización, el procesador está configurado además para:

generar información relativa a la configuración actual del segundo contexto de seguridad;
firmar criptográficamente la información con la segunda clave privada de identidad, $K_{2ID\ priv}$; y
donde el transceptor está configurado además para:
enviar la información y firma al primer contexto de seguridad.

[0083] En un modo de realización, el procesador está configurado además para:

generar el primer certificado criptográfico que comprende la información relativa a la configuración actual del segundo contexto de seguridad y firmar el primer certificado criptográfico con la segunda clave privada de identidad, $K_{2ID\ priv}$.

[0084] En un modo de realización, el transceptor está configurado además para:
recibir una segunda clave pública $K_{tenant\text{-}signpub}$ y un segundo certificado criptográfico firmado, el segundo certificado criptográfico comprendiendo información a partir de la cual puede validarse el origen de la segunda clave pública $K_{tenant\text{-}signpub}$, desde el primer contexto de seguridad;
y donde el procesador está configurado además para:
validar el origen de la segunda clave pública $K_{tenant\text{-}signpub}$.

[0085] En un aspecto adicional de la presente invención, se proporciona un dispositivo, que comprende:

una memoria de dispositivo, que almacena:

datos cifrados;
una lista de control de acceso correspondiente a los datos, especificando la lista de control de acceso que debe presentarse una credencial de uso válida para permitir un primer tipo de uso de los datos, y especificando que la credencial de uso debe comprender información a partir de la cual la expiración de la credencial de uso puede ser determinada y no debe haber expirado para permitir un primer tipo de uso de los datos; e
información a partir de la cual puede identificarse el origen de los datos.

[0086] En un modo de realización, la credencial de uso es un certificado de uso.

[0087] En un modo de realización, el dispositivo es un dispositivo criptográfico que comprende un segundo contexto de seguridad, para la cooperación con un dispositivo o dispositivos que comprenden un primer contexto de seguridad.

[0088] En un modo de realización, los datos comprenden una clave criptográfica, K_{tenant}.

[0089] La lista de control de acceso puede especificar que la credencial de uso es un certificado de uso que debe ser firmado por una clave privada $K_{tenant\text{-}signpriv}$ para permitir el uso de la clave criptográfica, K_{tenant}.

[0090] La lista de control de acceso puede especificar que la credencial de uso deba comprender información a partir de la cual pueda identificarse la clave criptográfica K_{tenant} correspondiente a la credencial de uso.

[0091] En un modo de realización, la clave criptográfica cifrada K_{tenant} está cifrada por una clave que no puede salir del segundo contexto de seguridad.

[0092] En un modo de realización, el dispositivo comprende además:

un procesador, configurado para

validar una credencial de uso recibida con respecto a la lista de control de acceso y validar que la credencial de uso no ha expirado;

permitir el primer tipo de uso de la clave criptográfica, K_{tenant}, en el segundo contexto de seguridad, con la condición de que la credencial de uso sea válida y no haya expirado.

[0093] En un modo de realización, se proporciona un método de transferencia de datos de un inquilino a un proveedor de servicios que comprende cifrar los datos con una clave pública de un par de claves generado mediante un dispositivo seguro dentro del sistema de proveedor de servicios. De este modo, no puede accederse a los datos por parte del proveedor de servicios durante la transmisión.

[0094] Los datos son generados con una lista de control de acceso correspondiente, que especifica que debe presentarse un certificado válido para permitir un uso concreto de los datos una vez almacenados. De este modo, el inquilino puede retener el control del uso de los datos, aunque hayan sido transferidos fuera del sistema de inquilino.

[0095] En un modo de realización, se proporciona un método de control del uso de datos almacenados de manera segura en el sistema de proveedor de servicios que comprende emitir una credencial de uso que tiene un tiempo de expiración a la parte que solicita el uso de los datos. La credencial de uso debe ser validada antes de que se permita el uso de los datos almacenados. Esto permite al inquilino permitir el uso de los datos almacenados durante un periodo de tiempo limitado.

[0096] En esta especificación, el término contexto de seguridad hace referencia a uno o más dispositivos de seguridad (por ejemplo, HSM), o particiones de un dispositivo de seguridad, que comparten al menos una clave privada y están configurados para salvaguardar y llevar a cabo un conjunto de funciones criptográficas.

[0097] En esta especificación, el término clave criptográfica hace referencia a un bloque de material criptográfico en bruto para su uso en operaciones criptográficas. Una lista de control de acceso correspondiente a la clave comprende información relativa a un conjunto de permisos que describen las operaciones para las que puede usarse el material de claves, por ejemplo, cifrado, descifrado o almacenamiento, y cualquier credencial que deba proporcionarse para habilitar los permisos. También asociada con la clave puede existir información relativa al tipo de clave que comprende datos que identifican el tipo de clave, incluyendo información que identifica, por ejemplo, los algoritmos con los que la clave puede usarse y su longitud, p.ej., el algoritmo Advanced Encryption Standard (AES) con una clave de longitud 256 bits, o el algoritmo RSA con una longitud de clave de 2048 bits.

[0098] En esta especificación, el término "verificar" puede utilizarse para hacer referencia a un método de comprobación de una firma criptográfica. El término "validar" puede utilizarse para hacer referencia a un método para comprobar que los datos son los esperados, o un método para comprobar que la firma es correcta y los datos son los esperados.

[0099] En esta especificación, el término "lista de control de acceso" hace referencia a uno o más permisos unidos a un objeto. Los permisos especifican qué operaciones están permitidas sobre el objeto, y las condiciones y/o credenciales requeridas para que se permita la operación. En los métodos descritos en esta especificación, las claves públicas pueden ser almacenadas en el primer contexto de seguridad o el segundo contexto de seguridad, o en medios que no son de confianza fuera del primer contexto de seguridad o el segundo contexto de seguridad si la integridad de la clave pública está protegida, por ejemplo, firmada mediante la clave de identidad del primer contexto de seguridad o el segundo contexto de seguridad. Esto significa que si la clave pública es manipulada, será detectado.

[0100] En los métodos descritos en esta especificación, la información enviada entre el primer contexto de seguridad y el segundo contexto de seguridad puede validarse mediante el uso de un certificado criptográfico. Por ejemplo, la información puede firmarse mediante una clave de firme privada que pertenezca al emisor, y la firma puede ser enviada junto con la información al receptor.

[0101] Los métodos descritos en esta especificación pueden ser métodos implementados por ordenador.

[0102] Puesto que algunos métodos según los modos de realización pueden implementarse por software, algunos modos de realización abarcan código informático proporcionado a un ordenador de propósito general en

cualquier medio portador adecuado. El medio portador puede comprender cualquier medio de almacenamiento no transitorio como un disquete, un CD ROM, un dispositivo magnético o un dispositivo de memoria programable, o cualquier medio transitorio como cualquier señal, por ejemplo, una señal eléctrica, óptica o de microondas.

Breve descripción de las figuras

[0103] Los dispositivos y métodos según los modos de realización no limitativos se describirán a continuación en relación con las figuras que acompañan en las cuales:

La figura 1(a) es una ilustración esquemática de una red que comprende un sistema de inquilino que comprende un dispositivo criptográfico según un modo de realización de la presente invención y un sistema de proveedor de servicios que comprende un dispositivo criptográfico según un modo de realización de la presente invención.

La figura 1(b) muestra una ilustración esquemática de un primer contexto de seguridad según un modo de realización de la presente invención y un segundo contexto de seguridad según un modo de realización de la presente invención;

La figura 2(a) es un diagrama de flujo que muestra un método para establecer la confianza entre el primer contexto de seguridad y el segundo contexto de seguridad, que es parte del método de transferencia de claves criptográficas según un modo de realización de la presente invención;

La figura 2(b) es un diagrama de flujo que muestra un método para validar la configuración del segundo contexto de seguridad en el primer contexto de seguridad, que es parte del método de transferencia de claves criptográficas según un modo de realización de la presente invención;

La figura 3 es una ilustración esquemática de un primer contexto de seguridad según un modo de realización de la presente invención y un segundo contexto de seguridad según un modo de realización de la presente invención, una vez que se ha establecido la confianza, y después de que se hayan generados las claves relevantes en cada contexto de seguridad;

La figura 4(a) es un diagrama de flujo que muestra un método para la transferencia de una clave de firma, $K_{tenant\text{-}sign}$ del primer contexto de seguridad al segundo contexto de seguridad, que es parte de un método de transferencia de claves criptográficas según un modo de realización de la presente invención;

La figura 4(b) es una ilustración de un método de registro de inquilino, que es parte de un método de transferencia de claves criptográficas según un modo de realización de la presente invención;

La figura 5 es una ilustración esquemática de un primer contexto de seguridad según un modo de realización de la presente invención y un segundo contexto de seguridad según un modo de realización de la presente invención, después de que la segunda clave pública, $K_{tenant\text{-}sign\ pub}$, haya sido intercambiada durante el proceso de transferencia de datos;

La figura 6(a) es un diagrama de flujo que muestra un método de transferencia de datos del primer contexto de seguridad al segundo contexto de seguridad según un modo de realización de la presente invención;

La figura 6(b) es un diagrama de flujo que muestra pasos adicionales de un método de transferencia de datos del primer contexto de seguridad al segundo contexto de seguridad según un modo de realización de la presente invención;

La figura 7(a) es una ilustración de un método de inscripción de clave, que es parte de un método de transferencia de claves criptográficas según un modo de realización de la presente invención;

La figura 7(b) es un diagrama de flujo de un método de transferencia de claves criptográficas según un modo de realización de la presente invención;

La figura 8(a) es una ilustración esquemática de un primer contexto de seguridad según un modo de realización de la presente invención y un segundo contexto de seguridad según un modo de realización de la presente invención, después de que la clave de inquilino K_{tenant} haya sido importada al segundo contexto de seguridad;

La figura 8(b) es una ilustración esquemática de una fuente de tiempo que puede ser alojada por el proveedor de servicios, el inquilino o un tercero independiente;

La figura 9 es un diagrama de flujo que muestra un método de registro de una fuente de tiempo en el segundo contexto de seguridad;

La figura 10 es un diagrama de flujo que muestra un método de registro de una fuente de tiempo en el primer contexto de seguridad;

La figura 11 es un diagrama de flujo que muestra un método de control del uso de datos según un modo de realización de la presente invención;

La figura 12 es un diagrama de flujo que muestra un método para generar un certificado de uso en el primer contexto de seguridad, que es parte de un método de control de uso de una clave criptográfica, K_{tenant} según un modo de realización de la presente invención;

La figura 13 es una ilustración de un método de control de uso de una clave criptográfica, K_{tenant} según un modo de realización de la presente invención;

La figura 14 es un diagrama de flujo de un método de control de uso de una clave criptográfica, K_{tenant} según un modo de realización de la presente invención.

Descripción detallada

[0104] La figura 1(a) es una ilustración esquemática de un sistema de inquilino 1 que comprende un dispositivo criptográfico según un modo de realización de la presente invención y un sistema de proveedor de servicios 3 que comprende un dispositivo criptográfico según otro modo de realización de la presente invención.

[0105] El proveedor de servicios puede ser un proveedor de servicios en la nube, por ejemplo. El proveedor de servicios proporciona almacenamiento de datos como claves criptográficas y procesamiento criptográfico de datos seguro a uno o más inquilinos. Por ejemplo, los inquilinos pueden usar la infraestructura criptográfica del sistema de proveedor de servicios 3 para aplicaciones como pagos, seguridad y regulación. El sistema de proveedor de servicios 3 comprende un servidor de aplicaciones de proveedor de servicios, configurado para llevar a cabo una o más aplicaciones como estas.

[0106] Para utilizar estos servicios, el sistema de inquilino 1 proporciona una clave criptográfica K_{tenant} al sistema de proveedor de servicios 3. La clave criptográfica K_{tenant} se almacena de manera segura en el sistema de proveedor de servicios 3 para su uso en tales aplicaciones.

[0107] El sistema de inquilino 1 comprende un primer contexto de seguridad 5 y el sistema de proveedor de servicios 3 comprende un segundo contexto de seguridad 7. Un contexto de seguridad puede ser un solo dispositivo de seguridad, por ejemplo, un módulo de seguridad de hardware, HSM. Alternativamente, puede ser dos o más dispositivos de seguridad, o una partición de un dispositivo de seguridad. El término contexto de seguridad se utiliza aquí para hacer referencia al dispositivo, dispositivos o partición de un dispositivo que forma un solo contexto de seguridad, a saber, que comparte al menos una clave privada y están configurados para salvaguardar y llevar a cabo un conjunto de funciones criptográficas. El primer contexto de seguridad 5 está protegido del resto del sistema del inquilino. El segundo contexto de seguridad 7 está protegido del resto del sistema de proveedor de servicios.

[0108] La clave criptográfica de inquilino K_{tenant} es proporcionada al segundo contexto de seguridad 7 en el sistema de proveedor de servicios 3. La clave criptográfica de inquilino K_{tenant} es entonces almacenada en el segundo contexto de seguridad 7 o es cifrada con una clave que no puede salir del segundo contexto de seguridad antes de ser almacenada en otro sitio en el sistema de proveedor de servicios 3.

[0109] Antes de proporcionar la clave criptográfica K_{tenant} al segundo contexto de seguridad 7, el inquilino puede autenticar y validar el segundo contexto de seguridad 7 a partir de un certificado de generación proporcionado por el segundo contexto de seguridad 7. El certificado de generación puede haberse generado en el momento de fabricación del dispositivo o dispositivos que son parte del segundo contexto de seguridad 7, por ejemplo. El inquilino confía en el fabricante, pero no en el proveedor de servicios. El certificado de generación autentica que el segundo contexto de seguridad 7 fue fabricado por el fabricante de confianza y, por tanto, es de confianza. Además, los parámetros y estados del segundo contexto de seguridad 7 pueden validarse, por ejemplo, a partir de la información contenida en el certificado de generación, y en un certificado de configuración adicional.

[0110] Un certificado de generación comprende información estática que es válida durante toda la vida útil del dispositivo. Un certificado de configuración comprende información sobre la configuración actual del dispositivo. La información de configuración es válida solo en el momento de generación del certificado de configuración y puede cambiar en una etapa posterior.

[0111] De este modo, el primer contexto de seguridad 5 establece la confianza con el segundo contexto de seguridad, antes de que comiencen las operaciones de transferencia de claves.

[0112] La clave criptográfica de inquilino K_{tenant} es cifrada con la mitad pública de un par de claves asimétrico generado en el segundo contexto de seguridad 7, antes de ser transferida al segundo contexto de seguridad 7. Un primer certificado criptográfico es emitido con el par de claves asimétrico generado en el segundo contexto de seguridad 7. En un modo de realización, el primer certificado criptográfico valida que el par de claves asimétricas fue generado en el segundo contexto de seguridad 7, que la mitad privada del par de claves asimétrico es efímera y que la mitad privada del par de claves asimétrico no puede salir del segundo contexto de seguridad 7. Esto permite que la clave criptográfica de inquilino K_{tenant} sea transferida al sistema de proveedor de servicios 3 de una manera segura frente a atacantes y frente al propio proveedor de servicios, esto es, frente al resto del sistema de proveedor de servicios 3 que se encuentra fuera del segundo contexto de seguridad 7, por ejemplo, el servidor de aplicaciones.

[0113] En un modo de realización, la clave criptográfica de inquilino K_{tenant} es almacenada entonces en el segundo contexto de seguridad 7. Alternativamente, la clave criptográfica de inquilino K_{tenant} es almacenada en otro lugar en el sistema de proveedor de servicios, por ejemplo, en el servidor de aplicaciones, cifrado mediante una clave que no puede salir del segundo contexto de seguridad 7.

[0114] Una lista de control de acceso (ACL) que corresponde a la clave criptográfica de inquilino K_{tenant} también es generada con la clave criptográfica de inquilino K_{tenant} en el primer contexto de seguridad 5. La ACL también es transferida al segundo contexto de seguridad 7 con la clave criptográfica de inquilino K_{tenant}. La ACL es almacenada con la clave criptográfica de inquilino K_{tenant}. El primer contexto de seguridad 5 ha establecido confianza con el segundo contexto de seguridad 7, y por tanto sabe que el segundo contexto de seguridad 7 aplicará las políticas contenidas en la ACL. De este modo, la ACL permite al inquilino conservar el control sobre la clave, incluso una vez que ha sido transferida al segundo contexto de seguridad 7.

[0115] En un modo de realización, la ACL especifica que la clave criptográfica de inquilino K_{tenant} puede almacenarse exclusivamente dentro del segundo contexto de seguridad 7. En un modo de realización alternativo, la ACL contiene una restricción de que la clave criptográfica de inquilino K_{tenant} puede ser almacenada exclusivamente con la condición de que sea cifrada para su almacenamiento mediante un clave que no puede salir del segundo contexto de seguridad 7. Esto garantiza que la clave criptográfica de inquilino K_{tenant} sea inaccesible para terceros y para el proveedor de servicios.

[0116] La ACL puede especificar que la clave critpográfica de inquilino K_{tenant} puede ser almacenada exclusivamente en la memoria no volátil siendo resistente a manipulaciones por terceros.

[0117] Además, la ACL especifica que debe presentarse una credencial de uso válida, por ejemplo, un certificado de uso, para permitir uno o más tipos de uso de la clave criptográfica de inquilino K_{tenant}. Por ejemplo, la ACL

puede requerir la presentación de un certificado firmado por la mitad privada de una clave asimétrica propiedad del inquilino para permitir la ejecución de determinadas operaciones criptográficas utilizando la clave de inquilino K_{tenant}. Esto garantiza que el tipo específico de operaciones que utilizan la clave no pueda ser utilizado si no es autorizado por el inquilino.

[0118] Aunque la clave criptográfica de inquilino K_{tenant} sea almacenada en el sistema de proveedor de servicios, el proveedor de servicios, esto es, el resto del sistema de proveedor de servicios 3 que está fuera del segundo contexto de seguridad 7 no puede acceder a la clave y la clave no puede utilizarse sin autorización del inquilino. Esto protege la clave criptográfica de inquilino K_{tenant} de un proveedor de servicios malicioso. También protege la clave criptográfica de inquilino K_{tenant} de agencias de seguridad que tienen jurisdicción sobre el proveedor de servicios, pero no el inquilino, por ejemplo.

[0119] También permite que múltiples inquilinos utilicen la misma infraestructura criptográfica en el proveedor de servicios. Múltiples inquilinos pueden almacenar claves en el mismo dispositivo de seguridad, puesto que cada clave criptográfica de inquilino K_{tenant} es inaccesible para otros inquilinos, y no puede ser utilizada sin autorización del inquilino correspondiente.

[0120] La lista de control de acceso puede especificar que la credencial de uso deba comprender información a partir de la cual pueda determinarse la expiración de la credencial de uso y no deba haber expirado para permitir el uso de la clave criptográfica, K_{tenant}. Así, el inquilino es capaz de especificar, en la credencial de uso, un periodo de expiración para su clave, tras el cual la clave no puede ser usada hasta que se proporciona otra autorización.

[0121] El tiempo de expiración puede calcularse en relación con una fuente de tiempo de referencia 2 que es de confianza para ambos el primer contexto de seguridad 5 y el segundo contexto de seguridad 7. La fuente de tiempo de referencia 2 puede ser alojada por el proveedor de servicios, el inquilino o un tercero independiente. La figura 1(a) muestra una ilustración esquemática de un modo de realización en el que la fuente de tiempo de referencia 2 es alojada por un tercero.

[0122] Aunque la descripción anterior está relacionada con la transferencia y almacenamiento de una clave criptográfica de inquilino, cualquier forma de datos puede ser transferida y almacenada de la misma manera. El método de transferencia de datos de un inquilino a un proveedor de servicios comprende cifrar los datos con una clave pública de un par de claves generado mediante un dispositivo seguro dentro del sistema de proveedor de servicios. De este modo, no puede accederse a los datos por parte del proveedor de servicios durante la transmisión. Los datos cifrados son firmados criptográficamente antes de la transferencia, para asegurar la autenticidad e integridad de los datos.

[0123] Los datos son generados con una lista de control de acceso correspondiente, que especifica que debe presentarse un certificado válido para permitir un uso concreto de los datos una vez almacenados. De este modo, el inquilino puede conservar el control del uso de los datos, aunque hayan sido transferidos fuera del sistema de inquilino.

[0124] Un método de control del uso de datos almacenados de manera segunda en el sistema de proveedor de servicios comprende emitir una credencial de uso que tiene un tiempo de expiración a la parte que solicita el uso de los datos. La credencial de uso debe ser validada antes de que se permita el uso de los datos almacenados. Esto faculta al inquilino a permitir el uso de los datos almacenados durante un periodo de tiempo limitado.

[0125] La figura 1(b) muestra una ilustración esquemática de un primer contexto de seguridad 5 según un modo de realización de la presente invención y un segundo contexto de seguridad 7 según otro modo de realización de la presente invención.

[0126] El primer contexto de seguridad 5 puede ser un solo dispositivo de seguridad, por ejemplo, un módulo de seguridad de hardware, HSM. Alternativamente, el primer contexto de seguridad 5 puede ser dos o más dispositivos de seguridad, o una partición de un dispositivo de seguridad. El primer contexto de seguridad 5 podría ser un HSM de baja potencia, bajo rendimiento y bajo coste, por ejemplo.

[0127] El segundo contexto de seguridad 7 puede ser un solo dispositivo de seguridad, por ejemplo, un módulo de seguridad de hardware. Alternativamente, el segundo contexto de seguridad 7 puede ser dos o más

dispositivos de seguridad, o una partición de un dispositivo de seguridad. El segundo contexto de seguridad 7 puede comprender un clúster de HSM de alto rendimiento.

[0128] De este modo, el primer contexto de seguridad 5 y el segundo contexto de seguridad 7 pueden comprender cada uno uno o más dispositivos criptográficos a prueba de manipulaciones o una partición de un dispositivo criptográfico a prueba de manipulaciones.

[0129] El primer contexto de seguridad 5 comprende una primera memoria de dispositivo 9. La primera memoria de dispositivo 9 está configurada para almacenar información criptográfica como claves, pares de claves y certificados. La primera memoria de dispositivo 9 puede incluir cualquier forma de memoria de dispositivo no volátil como *flash*, discos ópticos o discos duros magnéticos, por ejemplo. El primer contexto de seguridad 5 también comprende memoria volátil.

[0130] La primera memoria de dispositivo 9 puede estar protegida físicamente y ser resistente frente a manipulaciones de terceros, por ejemplo, mediante la inclusión de seguridad física como una membrana que cubre el dispositivo entero, que no puede ser eliminada sin destruir el hardware físico subyacente, haciéndolo así inutilizable.

[0131] Una clave de identidad asimétrica única K_{1ID} es almacenada en la primera memoria de dispositivo 9, con un certificado de generación firmado correspondiente $\{C_{1ID}\}_{Kman\ priv}$. K_{1ID} es una clave firmada utilizada para probar el origen de los datos y autenticidad. El certificado de generación C_{1ID} puede describir los parámetros públicos de la clave, por ejemplo, el certificado de generación C_{1ID} puede incluir información relativa al tipo de la clave y su longitud. El certificado de generación C_{1ID} comprende información que autentica que la clave de identidad K_{1ID} fue generada en el primer contexto de seguridad 5. Por ejemplo, el certificado de generación C_{1ID} puede comprender el *hash* de la mitad pública de K_{1ID} y estar firmado por la mitad privada de la clave asimétrica de fabricante, $K_{man\ priv}$.

[0132] El certificado de generación C_{1ID} puede incluir también información de estado, por ejemplo, información relativa a una identificación única del dispositivo, información que identifica al fabricante, la versión de hardware utilizada, el tipo de software utilizado, el número de serie de la unidad y las características/funcionalidad del modelo soportadas. El certificado de generación C_{1ID} es firmado por un fabricante de confianza tanto para el primer contexto de seguridad 5 como para el segundo contexto de seguridad 7. El certificado de generación es firmado criptográficamente con la mitad privada de una clave asimétrica de fabricante, $K_{man\ priv}$. El fabricante puede ser un tercero que fabricó el dispositivo o dispositivos de seguridad que forman el primer contexto de seguridad y el dispositivo o dispositivos de seguridad que forman el segundo contexto de seguridad. La mitad pública de la clave de fabricante de confianza $K_{man\ pub}$ también es almacenada en la primera memoria de dispositivo 9, o puede almacenarse fuera del primer contexto de seguridad 5 de manera que se proteja su integridad.

[0133] El segundo contexto de seguridad 7 comprende una segunda memoria de dispositivo 11. La segunda memoria de dispositivo 11 está configurada para almacenar información criptográfica como claves, pares de claves y certificados. La segunda memoria de dispositivo 11 puede incluir cualquier forma de memoria de dispositivo no volátil como *flash*, discos ópticos o discos duros magnéticos, por ejemplo. El segundo contexto de seguridad 5 también comprende memoria volátil.

[0134] La memoria de dispositivo puede estar protegida físicamente y ser resistente frente a manipulaciones por terceros, por ejemplo, mediante la inclusión de seguridad física como una membrana que cubre el dispositivo entero, que no puede ser eliminada sin destruir el hardware físico subyacente, haciéndolo así inutilizable.

[0135] Una clave de identidad asimétrica única K_{2ID} es almacenada en la segunda memoria de dispositivo 11, con un certificado de generación firmado correspondiente $\{C_{2ID}\}_{Kman\ priv}$. K_{2ID} es una clave de firma utilizada para probar el origen de los datos y autenticidad. El certificado de generación C_{2ID} puede describir los parámetros públicos de la clave, por ejemplo, el certificado de generación C_{2ID} puede incluir información relativa al tipo de la clave y su longitud. El certificado de generación C_{2ID} comprende información que autentica que la clave de identidad K_{2ID} fue generada en el segundo contexto de seguridad 7. Por ejemplo, el certificado de generación C_{2ID} puede incluir un *hash* de la mitad pública de K_{2ID}, y ser firmado por la mitad privada de la clave asimétrica de fabricante, $K_{man\ priv}$.

[0136] El certificado de generación C_{2ID} puede incluir también información de estado, por ejemplo, información relativa a una identificación única del dispositivo, información que identifica al fabricante, la versión de hardware, el tipo de software utilizado, el número de serie de la unidad y las características/funcionalidad del modelo soportadas. El certificado de generación C_{2ID} es firmado por el fabricante de confianza. El certificado de generación es firmado criptográficamente por la mitad privada de una clave asimétrica de fabricante, $K_{man\ priv}$ La mitad pública de la clave de fabricante de confianza $K_{man\ pub}$ también es almacenada en la segunda memoria de dispositivo 11, o puede almacenarse fuera del segundo contexto de seguridad 7 de manera que se proteja su integridad.

[0137] Tanto en el primer contexto de seguridad 5 como en el segundo contexto de seguridad 7, las claves criptográficas son almacenadas en la memoria de dispositivo en formato seguro y a prueba de manipulaciones.

[0138] El primer contexto de seguridad 5 y el segundo contexto de seguridad 7 pueden ser identificados de manera verificable utilizando certificados criptográficos, los certificados de generación firmados $\{C_{1ID}\}K_{man\ priv}$ y $\{C_{2ID}\}K_{man\ priv}$, que pueden ser generados en el momento de la fabricación. De este modo, cada uno es capaz de almacenar de manera segura su identidad de una manera que significa que no pueden ser imitados. Identificar el primer contexto de seguridad 5 y el segundo contexto de seguridad 7 permite comprobar el origen del dispositivo o dispositivos en cada contexto de seguridad. Cada dispositivo contiene la clave de identidad asimétrica única K_{ID} generada en la fábrica cuando fue fabricado, por ejemplo. Cada componente contiene también el certificado de generación de claves para la K_{ID} que es firmado utilizando una clave asimétrica conocida solo por el fabricante. La mitad pública de la clave de fabricante puede usarse como la raíz de confianza para autenticar los dispositivos auténticos.

[0139] Además, los parámetros y estado del primer contexto de seguridad y segundo contexto de seguridad pueden validarse de una manera no rechazable, a partir de información contenida en el certificado de generación, y a través del intercambio de certificados de configuración adicionales.

[0140] En un modo de realización, el primer contexto de seguridad 5 y el segundo contexto de seguridad 7 están configurados cada uno para generar un certificado de configuración, C_{1V} y C_{2V} respectivamente, que contiene información acerca de la configuración actual de los dispositivos establecida por el inquilino y el proveedor de servicios. La información de la configuración no puede incluirse en los certificados de generación, pues estos son generados en el momento de la fabricación, antes de que los dispositivos se distribuyan al inquilino y proveedor de servicios y sean configurados.

[0141] De este modo, una vez que los certificados de generación han sido intercambiados y se forma confianza entre los dos contextos de seguridad, puede intercambiarse información adicional relacionada con la configuración dinámica a través de la transferencia de datos de certificado firmado adicional. Los certificados de configuración, C_{1V} y C_{2V} respectivamente, son firmados por la mitad privada de la clave de identidad asimétrica única del contexto de seguridad correspondiente. El certificado de configuración es firmado por K_{IDpriv} para verificar la autenticidad, puesto que K_{IDpriv} es ahora de confianza para el otro contexto de seguridad. Los datos contenidos en el certificado de configuración pueden referirse a las opciones de implementación del administrador como ajustes de seguridad, versión de software, qué fuente de tiempo fiable es utilizada o si el HSM cree que ha habido un atento de manipularlo, por ejemplo.

[0142] El origen y el estado de un servicio define información suficiente por la que otros servicios pueden depositar su confianza. Esta información se intercambia en los certificados de generación y configuración.

[0143] Se confía en que el segundo contexto de seguridad aplique las normas especificadas en una ACL proporcionada al segundo contexto de seguridad y en que actualice sus certificados de estado de manera precisa. En un modo de realización, si el segundo contexto de seguridad no puede aplicar una norma al nivel especificado contenido en la ACL, entonces no llevará a cabo una operación y no se anunciará a si mismo o las claves que ha creado en apoyo de dichas normas.

[0144] Las claves de identidad del primer y segundo contexto de seguridad pueden instalarse en la fabricación, y el *hash* de estas claves puede ser firmado por una clave de fabricante $K_{man\ priv}$, y almacenado con la clave de identidad, probando así su procedencia.

[0145] Al ser capaz de identificar criptográficamente servicios de fuentes "de confianza", un inquilino es capaz de intercambiar su clave criptográfica con un servicio alojado por un canal de comunicación con una alta garantía de que todos los datos están protegidos y no son recuperables por ningún tercero, incluyendo el proveedor de servicios de alojamiento. Al garantizar que el dispositivo o dispositivos del proveedor de servicios en el segundo contexto de seguridad 7 son de confianza, a partir del certificado de generación, y que su configuración cumple la política de seguridad del inquilino, a partir del certificado de configuración, el inquilino puede transferir su clave sabiendo que la clave se almacenará de la manera especificada. La ACL enviada con la clave incluye políticas que especifican cómo debe almacenarse y utilizarse la clave. Entonces, el segundo contexto de seguridad 7 aplicará las políticas. El inquilino puede confiar en que el segundo contexto de seguridad 7 aplicará las políticas puesto que ha establecido confianza con el segundo contexto de seguridad 7. Establecer la confianza permite la transferencia segura y la ACL permite que el segundo contexto de seguridad 7 aplique una política una vez que está en posesión de la clave.

[0146] El primer contexto de seguridad 5 también comprende un transceptor 13. El transceptor 13 está configurado para transmitir y recibir paquetes de datos. Los paquetes de datos pueden transmitirse desde y recibirse en el primer transceptor 13, por ejemplo, a través de una conexión de internet o una conexión por cable directa entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7. Este enlace de comunicación puede no ser de confianza, sin embargo, el protocolo de transferencia de claves descrito en relación con la figura 6(a) a continuación proporciona protección de la clave frente a atacantes.

[0147] El primer contexto de seguridad 5 comprende además un primer procesador 17. El primer procesador 17 está configurado para llevar a cabo operaciones criptográficas, como generación de claves criptográficas y pares de claves criptográficas asimétricos, generación de certificados correspondientes a una clave criptográfica o par de claves criptográficas asimétrico, generación de listas de control de acceso correspondientes a una clave criptográfica, generación de certificados de uso correspondientes a una clave criptográfica, cifrado de un objeto con una clave criptográfica que es almacenada en la primera memoria de dispositivo 9, descifrado de un objeto cifrado con una clave criptográfica que es almacenada en la primera memoria de dispositivo 9, firmar criptográficamente un objeto con una clave criptográfica que es almacenada en la primera memoria de dispositivo 9, verificación de una firma criptográfica y validación de un objeto basándose en información almacenada en la primera memoria de dispositivo 9. El primer procesador 17 puede estar protegido físicamente.

[0148] En un modo de realización, el primer contexto de seguridad 5 comprende un procesador principal para llevar a cabo operaciones no criptográficas y el primer procesador 17 es un coprocesador, esto es, un componente independiente del procesador principal configurado para llevar a cabo solo las operaciones criptográficas. Alternativamente, el primer procesador 17 puede ser el procesador principal.

[0149] La generación de claves criptográficas y pares de claves criptográficas asimétricos puede comprender la generación de números aleatorios. El primer contexto de seguridad 5 puede comprender además una fuente de entropía aleatoria, para su uso en la generación de números aleatorios.

[0150] El segundo contexto de seguridad 7 comprende además un transceptor 15. El segundo transceptor 15 está configurado para transmitir y recibir paquetes de datos. Los paquetes de datos pueden transmitirse desde y recibirse en el segundo transceptor 15, por ejemplo, a través de una conexión a internet inalámbrica o una conexión por cable directa entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7.

[0151] El segundo contexto de seguridad 7 comprende además un segundo procesador 19. El segundo procesador 19 está configurado para llevar a cabo operaciones criptográficas, como generación de claves criptográficas y pares de claves criptográficas asimétricos, generación de certificados correspondientes a una clave criptográfica o par de claves criptográficas asimétrico, generación de listas de control de acceso correspondientes a una clave criptográfica, generación de certificados de uso correspondientes a una clave criptográfica, cifrado de un objeto con una clave criptográfica que es almacenada en la segunda memoria de dispositivo 11, descifrado de un objeto cifrado con una clave criptográfica que es almacenada en la segunda memoria de dispositivo 11, firmar criptográficamente un objeto con una clave criptográfica que es almacenada en la segunda memoria de dispositivo 11, verificación de una firma criptográfica y validación de un objeto basándose en información almacenada en la segunda memoria de dispositivo 11. El segundo procesador 19 puede estar protegido físicamente.

[0152] En un modo de realización, el primer contexto de seguridad 5 comprende un procesador principal para llevar a cabo operaciones no criptográficas y el primer procesador 17 es un coprocesador, esto es, un

componente independiente del procesador principal configurado para llevar a cabo solo las operaciones criptográficas. Alternativamente, el primer procesador 17 puede ser el procesador principal.

[0153] La generación de claves criptográficas y pares de claves criptográficas asimétricos puede comprender la generación de números aleatorios. El segundo contexto de seguridad 7 puede comprender además una fuente de entropía aleatoria para su uso en la generación de números aleatorios.

[0154] Un dispositivo HSM como puede utilizarse como parte del primer contexto de seguridad 5 o segundo contexto de seguridad 7 puede comprender una memoria de dispositivo, procesador, transceptor y fuente de entropía aleatoria como se ha describo con anterioridad. El HSM puede comprender propiedades de seguridad tanto físicas como no físicas. Las propiedades de seguridad no físicas incluyen el uso de cifrado, esto es, la inclusión en el dispositivo de software o un componente físico configurado para llevar a cabo el cifrado de los datos almacenados. Las propiedades físicas pueden incluir interruptores de seguridad accionados por acceso físico, y una membrana a prueba de manipulaciones que rodea el límite físico del dispositivo.

[0155] Los pares de claves asimétricos criptográficos analizados en esta solicitud pueden ser cualquier tipo de par de claves asimétrico que soporte la firma y verificación. Por ejemplo, cada uno del par de claves de fabricante K_{man}, la primera clave de identidad K_{1ID}, el segundo par de claves de identidad K_{2ID}, el par de claves de identidad de fuente de tiempo K_{TSID} y el par de claves de firma $K_{tenant\text{-}sign}$ pueden ser cualquiera de un par de claves RSA, DSA, o ECDSA, por ejemplo, donde RSA o DSA son el algoritmo para la firma y verificación.

[0156] Por ejemplo, para generar un par de claves RSA, una operación de generación puede llevarse a cabo por el primer procesador 17, segundo procesador 19 o tercer procesador 41 para generar un par de claves de salida que puede utilizarse por el algoritmo RSA para firmar datos.

[0157] Una fuente de entropía aleatoria puede utilizarse para generar números aleatorios, que a su vez son utilizados por el primer procesador 17, segundo procesador 19 o tercer procesador 41 para generar claves criptográficas y pares de claves criptográficas.

[0158] Los pares de claves asimétricos criptográficos en esta solicitud pueden ser cualquier tipo de pares de claves criptográficas asimétricos que soporte el cifrado y descifrado. Por ejemplo, el primer par de claves criptográficas K_{BLOB} puede ser un par de claves RSA o un par de claves que puede utilizarse en un algoritmo de Esquema Integrado de Cifrado (IES, por sus siglas en inglés).

[0159] La transferencia de certificados criptográficos y claves criptográficas entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7 descrita a continuación puede tener lugar a través de un canal seguro autenticado entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7 que es proporcionado y controlado por el proveedor de servicios. El canal seguro proporcionado por el proveedor de servicios puede ser proporcionado utilizando un balanceador de carga o cortafuegos. El uso de esta infraestructura mitiga los ataques como denegación de servicio.

[0160] Aunque el canal está protegido frente a terceros, está abierto a ataque por parte del proveedor de servicios, y, por tanto, no es de confianza para el inquilino para transferencia de claves criptográficas de alto valor. De este modo, se aplica seguridad por parte del inquilino mediante el cifrado de K_{tenant} y firma posterior de los datos cifrados enviados por el canal.

[0161] La figura 2(a) es un diagrama de flujo que muestra un método para establecer confianza entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7. El método para establecer confianza es parte de un método de transferencia de claves criptográficas según un modo de realización de la presente invención. El método para establecer confianza puede llevarse a cabo antes de que la clave criptográfica K_{tenant} sea generada, por ejemplo, o puede llevarse a cabo después de que la clave criptográfica se haya generado, pero antes de cualquier intercambio de claves criptográficas entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7, por ejemplo.

[0162] En el paso S201, la mitad pública de la clave de identidad del primer contexto de seguridad, $K_{1ID\ pub}$, y el certificado de generación $\{C_{1ID}\}_{Kman\ priv}$, son enviados desde el primer contexto de seguridad 5 al segundo contexto de seguridad 7. El primer transceptor 13 en el primer contexto de seguridad 5 es configurado para enviar la mitad pública de la clave de identidad del primer contexto de seguridad, $K_{1ID\ pub}$, y el certificado de

generación $\{C_{1ID}\}_{Kman\ priv}$, al segundo transceptor 15 en el segundo contexto de seguridad 7. La información relativa al estado del dispositivo o dispositivos en el primer contexto de seguridad 5 puede enviarse en el mismo mensaje. La información relativa al estado del dispositivo o dispositivos también es incluida en el certificado de generación en este caso, y puede utilizarse por el receptor para validar la información de estado contenida en el mensaje.

[0163] El certificado de generación es inmutable, de este modo solo contiene información que está disponible en el momento de la fabricación. Puede incluirse información relacionada con la configuración actual del dispositivo, por ejemplo, la dirección IP o estado de protección antimanipulación, en el certificado de configuración. La información de configuración puede enviarse al mismo tiempo que el certificado de generación o después del certificado de generación. Sin embargo, el certificado de generación es generado y firmado en el momento de la fabricación, mientras que el certificado de configuración es generado en el momento de transferencia de claves, y es firmado por $K_{1ID\text{-}priv}$. El certificado de configuración puede verificarse solo después de que el certificado de generación haya sido verificado.

[0164] En el paso S202, la firma del certificado de generación $\{C_{1ID}\}$ $K_{man\ priv}$ es verificada en el segundo contexto de seguridad 7. El segundo procesador 19 en el segundo contexto de seguridad 7 es configurado para verificar la firma del certificado de generación $\{C_{1ID}\}_{Kman\ priv}$. El certificado de generación es verificado utilizando la mitad pública de la clave de fabricante de confianza $K_{man\ pub}$ que es almacenada en la memoria de dispositivo 11. El segundo procesador 19 es configurado para llevar a cabo un algoritmo de verificación de firma que, dado el mensaje firmado $\{C_{1ID}\}_{Kman\ priv}$ y la clave pública $K_{man\ pub}$ acepte o rechace la declaración de autenticidad del mensaje.

[0165] La autenticidad de la mitad pública de la clave de identidad del primer contexto de seguridad, $K_{1ID\ pub}$ es validada en el segundo contexto de seguridad 7. El segundo procesador 19 en el segundo contexto de seguridad 7 es configurado para validar la mitad pública de la clave de identidad del primer contexto de seguridad, $K_{1ID\ pub}$. En un modo de realización en el que el certificado de generación C_{1ID} comprende un *hash* de la mitad pública de la clave de identidad del primer contexto de seguridad, $K_{1ID\ pub}$, la autenticidad se valida mediante el cálculo del *hash* de la mitad pública de la clave de identidad del primer contexto de seguridad, $K_{1ID\ pub}$, y validando si se corresponde con el contenido en su certificado de generación C11D.

[0166] En un modo de realización, el certificado de generación C_{1ID} comprende el *hash* de la mitad pública de K_{1ID} y es firmado por la mitad privada de la clave asimétrica de fabricante, $K_{man\ priv}$ Paso S202 comprende: calcular el *hash* de los datos recibidos enviados en el mensaje, en este caso el *hash* de $K_{1ID\ pub}$; introducir la firma recibida en el algoritmo de verificación, que puede ser una operación criptográfica, junto con la mitad pública de la clave de fabricante y verificar el resultado; comparar el *hash* calculado con el contenido en el resultado del algoritmo de verificación para determinar si son iguales.

[0167] En el paso S203, si se incluye en el mensaje información de estado, el segundo contexto de seguridad 7 valida que el estado del dispositivo o dispositivos cumple los requisitos. Alternativamente, la información de estado no se incluye en el certificado de generación, y el segundo contexto de seguridad 7 no valida el estado del primer contexto de seguridad 5. El segundo contexto de seguridad 7 no transfiere ninguna información segura al primer contexto de seguridad 5, de este modo no es necesario que la información de estado del primer contexto de seguridad 5 sea validada.

[0168] Si la firma es verificada y la información de estado es validada, la mitad pública de la clave de identidad del primer contexto de seguridad, $K_{1ID\ pub}$, es almacenada en la segunda memoria de dispositivo 11 del segundo contexto de seguridad 7. Alternativamente, puede protegerse la integridad de la mitad pública de la clave de identidad del primer contexto de seguridad, $K_{1ID\ pub}$ por el segundo contexto de seguridad 7 y puede ser almacenada en un almacenamiento no de confianza fuera del segundo contexto de seguridad 7. El segundo contexto de seguridad 7 puede firmar la mitad pública de la clave de identidad del primer contexto de seguridad, $K_{1ID\ pub}$, y los datos que indican que esta es una clave pública de una fuente de confianza, utilizando $K_{2ID\ priv}$ para el almacenamiento. Alternativamente, puede cifrarlos usando otra clave secreta. En estos casos, puede utilizarse una memoria de dispositivo no de confianza, que a menudo tiene una capacidad mayor que la memoria de dispositivo dentro del segundo contexto de seguridad 7, mientras que se mantiene la confianza en la clave.

[0169] Si la firma no es verificada o la información de estado no es validada, se devuelve un error al primer contexto de seguridad, por ejemplo, se envía un mensaje indicando "Acceso denegado". En este momento, se termina la comunicación entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7.

[0170] En el paso S204, la mitad pública de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ pub}$, y el certificado de generación $\{C_{2ID}\}_{Kman\ priv}$, son enviados desde el segundo contexto de seguridad 7 al primer contexto de seguridad 5. El segundo transceptor 15 en el segundo contexto de seguridad 7 es configurado para enviar la mitad pública de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ pub}$, y el certificado de generación $\{C_{2ID}\}_{Kman\ priv}$, al primer transceptor 13 en el primer contexto de seguridad 5. La información relativa al estado del dispositivo o dispositivos en el segundo contexto de seguridad 7 puede enviarse en el mismo mensaje. La información relativa al estado del dispositivo o dispositivos también es incluida en el certificado de generación en este caso, para validar la información de estado. De nuevo, el certificado de generación es inmutable, de este modo solo contiene información que está disponible en el momento de la fabricación. Puede incluirse información relacionada con la configuración actual del dispositivo, por ejemplo, la dirección IP o estado de protección antimanipulación, en el certificado de configuración. La información de configuración puede enviarse al mismo tiempo que el certificado de generación, o después del certificado de generación, por ejemplo, en el paso S604 como parte del primer certificado criptográfico C_{BLOB}. Sin embargo, el certificado de generación es generado y firmado en el momento de la fabricación, mientras que el certificado de configuración es generado en el momento de transferencia de claves, y es firmado por $K_{2ID\text{-}priv}$. El certificado de configuración puede verificarse solo después de que el certificado de generación haya sido verificado.

[0171] En el paso S205, la firma del certificado de generación $\{C_{2ID}\}\ K_{man\ priv}$ es verificada en el primer contexto de seguridad 5. El primer procesador 17 en el primer contexto de seguridad 5 es configurado para verificar el certificado de generación $\{C_{2ID}\}\ K_{man\ priv}$. La firma es verificada utilizando la mitad pública de la clave de fabricante de confianza $K_{man\ pub}$ almacenada en la memoria de dispositivo 9. El primer procesador 17 es configurado para llevar a cabo un algoritmo de verificación de firma que, dado el mensaje firmado $\{C_{2ID}\}\ K_{man\ priv}$ y la clave pública $K_{man\ pub}$ acepte o rechace la declaración de autenticidad del mensaje. Esto permite que el primer contexto de seguridad 5 valide el dispositivo del fabricante en el segundo contexto de seguridad 7, mediante la verificación de la firma.

[0172] La autenticidad de la mitad pública de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ pub}$ es validada en el primer contexto de seguridad 5. El primer procesador 17 en el primer contexto de seguridad 5 es configurado para validar la mitad pública de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ pub}$. En un modo de realización en el que el certificado de generación C_{2ID} comprende un *hash* de la mitad pública de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ pub}$, la autenticidad se valida mediante el cálculo del *hash* de la mitad pública de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ pub}$, y validando si se corresponde con el contenido en su certificado de generación C21D.

[0173] En el paso S206, si se incluye en el mensaje información de estado, el primer contexto de seguridad 5 valida que el estado del dispositivo o dispositivos cumple los requisitos.

[0174] Si la firma es verificada y la información de estado es validada, la mitad pública de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ pub}$, es almacenada en la primera memoria de dispositivo 9 del primer contexto de seguridad 5. Alternativamente, puede protegerse la integridad de la mitad pública de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ pub}$ por el primer contexto de seguridad 5 y puede ser almacenada en un almacenamiento no de confianza fuera del primer contexto de seguridad 5. El primer contexto de seguridad 5 puede firmar la mitad pública de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ pub}$, y los datos que indican que esta es una clave pública de una fuente de confianza, utilizando $K_{1ID\ priv}$ para el almacenamiento. Alternativamente, puede cifrarlos usando otra clave secreta. En estos casos, puede utilizarse una memoria de dispositivo no de confianza, que a menudo tiene una capacidad mayor que la memoria de dispositivo dentro del primer contexto de seguridad 5, mientras que se mantiene la confianza en la clave.

[0175] Si la firma no es verificada o la información de estado no es validada, se devuelve un error al segundo contexto de seguridad 7, por ejemplo, se envía un mensaje indicando "Acceso denegado". En este momento, se termina la comunicación entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7.

[0176] La figura 2(b) es un diagrama de flujo que muestra un método para validar la configuración del segundo contexto de seguridad 7 en el primer contexto de seguridad 5, que es parte de un método de transferencia de clave criptográfica según un modo de realización de la presente invención. En este método, la configuración del segundo contexto de seguridad 7 puede ser validada. En un modo de realización, puede utilizarse también un método similar para validar la configuración del primer contexto de seguridad 5 en el segundo contexto de seguridad 7. Alternativamente, el segundo contexto de seguridad 7 no valida la configuración del primer contexto de seguridad 5. El segundo contexto de seguridad 7 no transfiere ninguna información segura al primer contexto

de seguridad 5, de este modo no es necesario que la configuración del primer contexto de seguridad 5 sea validada.

[0177] La información de configuración es generada por el segundo contexto de seguridad 7 en el paso S211. La información de configuración puede incluir información relativa a la configuración específica aplicada por el administrador. Esto puede incluir información relativa a las operaciones criptográficas que son soportadas, las claves de cifrado que son utilizadas, y/o la versión de software de la unidad, por ejemplo. La información de configuración puede comprender información que indica que el primer contexto de seguridad 5 ha sido configurado para utilizar el algoritmo AES para cifrar claves de inquilino cuando no esté dentro del segundo contexto de seguridad 7, por ejemplo. La información de configuración puede comprender además información relativa a las opciones de implementación del administrador como ajustes de seguridad, qué fuente de tiempo de confianza es utilizada o si el segundo contexto de seguridad 7 cree que ha habido un intento de manipular el dispositivo.

[0178] En el paso S212, la información de configuración es firmada por la mitad privada de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ priv}$, produciendo un certificado de configuración C_{2V}. La mitad privada de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ priv}$ es almacenada en el segundo contexto de seguridad 7 y un administrador no puede acceder a ella. La firma del certificado de configuración C_{2V} con la mitad privada de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ priv}$ significa que la información de configuración no puede ser subvertida.

[0179] En el paso S213, la información de configuración y certificado de configuración C_{2V} es enviado desde el segundo contexto de seguridad 7 al primer contexto de seguridad 5. Esto puede enviarse a la vez que $K_{2ID\ pub}$ y $\{C_{2ID}\}$ $K_{man\ priv}$, en el paso S204, por ejemplo. Alternativamente, la información de configuración puede incluirse en el primer certificado criptográfico descrito en relación con la Figura 6(a), y la información de configuración puede enviarse al mismo tiempo que el primer certificado criptográfico C_{BLOB}. El segundo transceptor 15 en el segundo contexto de seguridad 7 es configurado para enviar la información de configuración y el certificado de configuración C_{2V} al primer transceptor 13 en el primer contexto de seguridad 5.

[0180] En el paso S214, el certificado de configuración firmado C_{2V} es verificado en el primer contexto de seguridad 5. El primer procesador 17 en el primer contexto de seguridad 5 es configurado para verificar el certificado de configuración firmado C_{2V}. El certificado de configuración firmado C_{2V} es verificado utilizando la mitad pública de la segunda clave de identidad $K_{2ID\ pub}$ almacenada en la memoria de dispositivo 9, tras ser recibido y procesado en los pasos del S204 a S206. El primer procesador 17 es configurado para llevar a cabo un algoritmo de verificación de firma que, dado el certificado de configuración firmado C_{2V} y la clave pública $K_{2ID\ pub}$ acepte o rechace la declaración de autenticidad del mensaje. Esto permite que el primer contexto de seguridad 5 pruebe que la información de configuración ha sido generada por un dispositivo conocido.

[0181] En el paso S215, el primer contexto de seguridad valida que la información de configuración cumple sus requisitos.

[0182] En un modo de realización, la información de configuración es solicitada y comprobada inmediatamente antes de la transferencia de K_{tenant} al segundo contexto de seguridad 7. Esto asegura que se valida información de configuración actualizada.

[0183] En un modo de realización, la información de configuración y un certificado de configuración son generados también y enviados por el primer contexto de seguridad 5 de manera similar. La información de configuración puede comprender información relativa a la configuración específica aplicada por el administrador. La información de configuración es firmada por la mitad privada de la clave de identidad del primer contexto de seguridad 5 y enviada al segundo contexto de seguridad 7, que valida que la configuración del primer contexto de seguridad 5 cumple sus requisitos.

[0184] En el método descrito anteriormente, el inquilino se registra él mismo en el proveedor de servicios. El registro se lleva a cabo en forma de autenticación mutua de las dos partes en un medio inseguro. La autenticación mutua del primer contexto de seguridad 5 y el segundo contexto de seguridad 7 se lleva a cabo utilizando las claves de identidad asimétricas únicas. Las mitades públicas de las claves de identidad son intercambiadas junto con sus certificados de generación correspondientes. Cada contexto de seguridad valida el certificado de generación del otro comprobando que el certificado contiene el *hash* de la mitad pública de la clave

de identidad y que el certificado ha sido realmente creado por un fabricante de confianza. El certificado de generación de la clave de identidad puede denominarse un permiso. Utilizando la raíz de confianza compartida establecida, el primer contexto de seguridad 5 y segundo contexto de seguridad 7 establecen una comunicación de red autentificada y segura con un socio fiable y verificable. El primer contexto de seguridad 5 y el segundo contexto de seguridad 7 validan cada uno de manera criptográfica que el otro fue construido por un fabricante de confianza.

[0185] El paso S205 de verificar el certificado de generación firmado $\{C_{2ID}\}$ $K_{man\ priv}$ en el primer contexto de seguridad utilizando $K_{man\ pub}$ verifica que el segundo contexto de seguridad 7 es de un origen de confianza conocido.

[0186] La figura 3 es una ilustración esquemática del sistema de inquilino 1 y sistema de proveedor de servicios 3 tras haberse establecido confianza, y después de que se hayan generado las claves relevantes en cada contexto de seguridad.

[0187] La primera memoria de dispositivo 9 en el primer contexto de seguridad 5 también almacena la mitad pública de la clave de identidad del segundo contexto de seguridad $K_{2ID\ pub}$. Alternativamente, esta clave puede almacenarse fuera del primer contexto de seguridad 5 de manera que se proteja su integridad. La primera memoria de dispositivo 9 también almacena la clave de inquilino K_{tenant}, generada en el paso S601 descrito a continuación, y el segundo par de claves $K_{tenant\text{-}sign}$, generado en el paso S401 descrito a continuación.

[0188] La segunda memoria de dispositivo 11 en el segundo contexto de seguridad 7 también almacena la mitad pública de la clave de identidad del primer contexto de seguridad $K_{1ID\ pub}$. Alternativamente, esta clave puede almacenarse fuera del primer contexto de seguridad 5 de manera que se proteja su integridad. La segunda memoria de dispositivo 1 también almacena el primer par de claves criptográficas y un primer certificado criptográfico generado en el paso S602 descrito a continuación.

[0189] La figura 4(a) es un diagrama de flujo que muestra un método de transferencia de una clave de firma, $K_{tenant\text{-}sign}$ del primer contexto de seguridad 5 al segundo contexto de seguridad 7, que es parte de un método de transferencia de claves criptográficas según un modo de realización de la presente invención. En un modo de realización, el método de transferencia de la clave de firma $K_{tenant\text{-}sign}$ se lleva a cabo antes de que la clave criptográfica K_{tenant} se envíe al segundo contexto de seguridad 7. El método de transferencia de la clave de firma $K_{tenant\text{-}sign}$ puede llevarse a cabo después de que se haya generado la clave criptográfica K_{tenant}.

[0190] En el paso S401, el par de claves criptográficas asimétrico $K_{tenant\text{-}signpub}$ y $K_{tenant\text{-}signpriv}$ y certificado correspondiente $C_{tenant\text{-}sign}$ son generados en el primer contexto de seguridad 5. El par de claves criptográficas asimétricas $K_{tenant\text{-}signpub}$ y $K_{tenant\text{-}signpriv}$ se denominan la segunda clave pública y la segunda clave privada y el certificado correspondiente $C_{tenant\text{-}sign}$ se denomina el segundo certificado criptográfico. El primer procesador 17 en el primer contexto de seguridad 5 es configurado para generar el par de claves criptográficas asimétrico $K_{tenant\text{-}signpub}$ y $K_{tenant\text{-}signpriv}$ y certificado correspondiente $C_{tenant\text{-}sign}$. El segundo certificado criptográfico, $C_{tenant\text{-}sign}$ puede comprender el *hash* firmado de la segunda clave pública $K_{tenant\text{-}signpub}$.

[0191] En el paso S402, el segundo certificado criptográfico, $C_{tenant\text{-}sign}$ es firmado criptográficamente con la mitad privada de la clave de identidad del primer contexto de seguridad, $K_{1ID\ priv}$. El primer procesador 17 está configurado para firmar criptográficamente el segundo certificado criptográfico, $C_{tenant\text{-}sign}$ con la mitad privada de la clave de identidad del primer contexto de seguridad, $K_{1ID\ priv}$.

[0192] El segundo certificado criptográfico $C_{tenant\text{-}sign}$ comprende así información a partir de la cual puede validarse el origen de la segunda clave pública $K_{tenant\text{-}signpub}$. La información a partir de la cual el origen de la segunda clave pública $K_{tenant\text{-}signpub}$ puede validarse comprende el *hash* firmado de la segunda clave pública $K_{tenant\text{-}signpub}$. El segundo certificado criptográfico $C_{tenant\text{-}sign}$ comprende un *hash* de la segunda clave pública $K_{tenant\text{-}signpub}$ y es firmado con la mitad privada de la clave de identidad del primer contexto de seguridad, $K_{1ID\ priv}$, que permite que se valide el origen de la segunda clave pública $K_{tenant\text{-}signpub}$.

[0193] En el paso S403, la segunda clave pública $K_{tenant\text{-}signpub}$ y el segundo certificado criptográfico $\{C_{tenant\text{-}sign}\}$ $K_{1ID\ priv}$ son enviados al segundo contexto de seguridad 7. El primer transceptor 13 está configurado para enviar la segunda clave pública $K_{tenant\text{-}signpub}$ y el segundo certificado criptográfico $\{C_{tenant\text{-}sign}\}$ $K_{1ID\ priv}$ al segundo contexto de seguridad 7.

[0194] En el paso S404, el segundo certificado criptográfico $\{C_{tenant\text{-}sign}\}_{K1ID\ priv}$ es verificado en el segundo contexto de seguridad 7. El segundo procesador 19 en el segundo contexto de seguridad 7 es configurado para verificar el segundo certificado $\{C_{tenant\text{-}sign}\}_{K1ID\ priv}$. El segundo certificado es verificado utilizando la mitad pública de la clave de identidad del primer contexto de seguridad, $K_{1ID\ pub}$. El segundo procesador 19 es configurado para llevar a cabo un algoritmo de verificación de firma que, dado el mensaje firmado $\{C_{tenant\text{-}sign}\}_{K1ID\ priv}$ y la clave pública $K_{1ID\ pub}$ acepte o rechace la declaración de autenticidad del mensaje.

[0195] La autenticidad de la segunda clave pública $K_{tenant\text{-}signpub}$ es validada entonces en el segundo contexto de seguridad 7. El segundo procesador 19 en el segundo contexto de seguridad 7 es configurado para validar la segunda clave pública $K_{tenant\text{-}signpub}$. En un modo de realización en el que el segundo certificado criptográfico $C_{tenant\text{-}sign}$ comprende un *hash* de la segunda clave pública $K_{tenant\text{-}signpub}$, la autenticidad de la segunda clave pública $K_{tenant\text{-}signpub}$ es validada calculando el *hash* de la segunda clave pública $K_{tenant\text{-}signpub}$, y validando que se corresponde con el contenido en el segundo certificado criptográfico $C_{tenant\text{-}sign}$.

[0196] Si la firma es verificada y la segunda clave pública es validada, la segunda clave pública $K_{tenant\text{-}signpub}$, es almacenada en la segunda memoria de dispositivo 11 del segundo contexto de seguridad 7. Alternativamente, puede protegerse su integridad por el segundo contexto de seguridad 7 y almacenarse en un almacenamiento no de confianza fuera del segundo contexto de seguridad 7.

[0197] Si la firma no es verificada o la segunda clave pública no es validada, se devuelve un error al primer contexto de seguridad 5, por ejemplo, se envía un mensaje indicando "Acceso denegado". En este momento, se termina la comunicación entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7.

[0198] En el método descrito anteriormente, una vez se establece la confianza con éxito, el primer contexto de seguridad 5 genera una clave asimétrica, $K_{tenant\text{-}sign}$, y envía la mitad pública incluyendo un certificado firmado por la mitad privada de K_{1ID} al segundo contexto de seguridad 7. El segundo contexto de seguridad 7 valida el certificado y almacena la mitad pública de $K_{tenant.sign}$ en la segunda memoria de dispositivo 11 o en otro lugar en un formato seguro a prueba de manipulaciones para su uso posterior. De este modo, el primer contexto de seguridad 5 en el sistema de inquilino genera una clave asimétrica, $K_{tenant\text{-}sign}$, y envía la mitad públcia al segundo contexto de seguridad para su almacenamiento y uso posterior.

[0199] La figura 4(b) es una ilustración esquemática de un método de registro de inquilino, que es parte de un método de transferencia de claves criptográficas según un modo de realización de la presente invención. El método comprende generar la clave criptográfica de inquilino K_{tenant} como se describe en relación con el paso S601 a continuación, establecer confianza como se ha descrito en relación con la figura 2(a) anteriormente, y generar e intercambiar la segunda clave pública como se ha descrito en relación con la figura 4(a) anteriormente.

[0200] Cada recuadro vertical en el diagrama representa la entidad incluida, es decir, el primer contexto de seguridad 5, el segundo contexto de seguridad 7 y la fuente de tiempo 3 con el transcurso del tiempo, aumentando el tiempo en la dirección hacia bajo. Los bloques en los que se originan y donde terminan flechas y bucles indican la duración de un proceso concreto. Por ejemplo, el segundo contexto de seguridad 7 recibe la mitad pública de la clave de identidad del primer contexto de seguridad $K_{1ID\ pub}$ y certificado de generación correspondiente. Esto comienza un proceso en el segundo contexto de seguridad 7. El siguiente paso del proceso es validar el certificado y entonces enviar una respuesta al primer contexto de seguridad 5, esto es, un mensaje de error si el certificado no es validado, o un mensaje que contenga su propia clave de identidad pública y certificado si el certificado es validado. Este es el final del proceso concreto.

[0201] Los bucles indican acciones que tienen lugar de manera interna a un proceso, por ejemplo, la validación, que no requiere interacción con ninguna otra entidad. Las líneas que cruzan entre entidades indican comunicación entre las entidades.

[0202] La clave criptográfica K_{tenant} es generada en el primer contexto de seguridad 5. La segunda clave criptográfica K_{tenant} es generada entonces en el primer contexto de seguridad 5. La mitad pública de la clave de identidad $K_{1ID\ pub}$ y el certificado firmado $\{C_{1ID}\}_{Kman\ priv}$ se envían entonces desde el primer contexto de seguridad 5 al segundo contexto de seguridad 7 y se validan en el segundo contexto de seguridad 7. La mitad pública de la clave de identidad $K_{2ID\ pub}$ y el certificado firmado $\{C_{2ID}\}_{Kman\ priv}$ se envían entonces desde el segundo contexto de seguridad 7 al primer contexto de seguridad 5 y se validan en el primer contexto de seguridad 5. La segunda

clave criptográfica $K_{tenant\text{-}sign\ pub}$ y certificado firmado $\{C_{tenant\text{-}sign}\}_{K1ID\ priv}$ son enviados al segundo contexto de seguridad 7 donde son validados y almacenados.

[0203] La figura 5 es una ilustración esquemática del sistema de inquilino 1 y del sistema de proveedor de servicios 3 después de que la segunda clave pública, $K_{tenant\text{-}sign\ pub}$, haya sido intercambiada durante el proceso de transferencia de datos analizado en relación con la figura 6(a) a continuación.

[0204] En un modo de realización, K_{blob} y C_{blob} son transitorios, y una vez que K_{tenant} ha sido transferida, son eliminados del segundo contexto de seguridad 7.

[0205] La segunda memoria de dispositivo 11 en el segundo contexto de seguridad 7 también almacena la mitad pública de la segunda clave $K_{tenant\text{-}sign\ pub}$. Alternativamente, esta clave puede almacenarse fuera del primer contexto de seguridad 5 de manera que se proteja su integridad.

[0206] La figura 6(a) es un diagrama de flujo que muestra un método de transferencia de datos del primer contexto de seguridad 5 al segundo contexto de seguridad 7 según un modo de realización de la presente invención. En un modo de realización mostrado en la figura 6(a), los datos son una clave criptográfica, K_{tenant}

[0207] Una vez que el sistema de inquilino se ha registrado en el sistema de proveedor de servicios, el primer contexto de seguridad 5 conecta con el segundo contexto de seguridad 7 a través de una conexión segura autenticada e inicia el proceso de transferencia de clave, o importación.

[0208] En el paso S601, la clave criptográfica, K_{tenant}, y una lista de control de acceso correspondiente, ACL, son generadas en el primer contexto de seguridad 5. El primer procesador 17 en el primer contexto de seguridad 5 es configurado para generar la clave criptográfica, K_{tenant}, y lista de control de acceso correspondiente.

[0209] De este modo, el primer contexto de seguridad 5 genera una clave, K_{tenant}, que prestará al proveedor de servicios. K_{tenant} es generada dentro de un dispositivo seguro en el primer contexto de seguridad 5 con una lista de control de acceso (ACL).

[0210] La ACL especifica que una credencial de uso válida, por ejemplo, un certificado de uso, debe presentarse para permitir un primer tipo de uso de la clave. El primer tipo de uso puede ser una operación criptográfica, por ejemplo. La ACL describe cómo puede usarse la clave, cualquier restricción sobre su uso y qué credenciales deben proporcionarse para que se permita cada operación.

[0211] En un modo de realización alternativo, la clave criptográfica, K_{tenant}, no es generada en el primer contexto de seguridad 5, sino que es generada fuera del primer contexto de seguridad 5 y después proporcionada al primer contexto de seguridad 5.

[0212] En un modo de realización alternativo, en lugar de la clave criptográfica, K_{tenant}, algún otro tipo de dato es generado en o proporcionado al primer contexto de seguridad 5. A continuación, se genera una lista de control de acceso correspondiente a los datos, que especifica que debe presentarse una credencial de uso válida para permitir un primer tipo de uso de los datos. El primer tipo de uso puede ser leer los contenidos del archivo de datos, por ejemplo.

[0213] En la descripción a continuación, los métodos y aparatos se describen en relación con la transferencia y concesión de una clave de inquilino, sin embargo, se entiende que algún otro tipo de dato puede ser sustituido por la clave de inquilino, y transferido y concedido del mismo modo.

[0214] La ACL puede comprender uno o más permisos, o políticas. Cada permiso puede regular un uso concreto de la clave. Por ejemplo, un primer permiso regula cómo puede almacenarse la clave, un segundo permiso regula cómo puede usarse la clave para cifrado, un tercer permiso regula cómo puede usarse la clave para descifrado, etcétera.

[0215] La ACL también comprende credencial(es) asociada(s) con un permiso concreto. Las credenciales especifican qué debe proporcionarse para autorizar un permiso concreto. Algunos permisos pueden no tener una credencial asociada, por ejemplo, el permiso de almacenamiento.

[0216] El inquilino ha validado que el segundo contexto de seguridad 7 se adhiere a los requisitos en la ACL antes de que la clave sea transferida, como se describe en relación con las figuras 2(a) y (b). El inquilino valida que el segundo contexto de seguridad 7 es fabricado por un fabricante de confianza. El inquilino puede validar también que la configuración actual del segundo contexto de seguridad 7 cumple los requisitos de seguridad del inquilino. Al validar que el segundo contexto de seguridad 7 es de confianza y cumple los requisitos del inquilino, el inquilino puede asegurar que el segundo contexto de seguridad 7 aplicará las políticas/permisos contenidos en la ACL.

[0217] La lista de control de acceso especifica que una credencial de uso válida, por ejemplo, un certificado de uso, debe presentarse para permitir un determinado uso o usos de la clave criptográfica, K_{tenant}. De este modo, la ACL de K_{tenant} puede requerir que se presente un certificado válido cada vez que la clave es utilizada para cifrado, por ejemplo. Los permisos relacionados con estos usos, por tanto, tienen credenciales asociadas, por ejemplo, el certificado de uso.

[0218] Un inquilino puede especificar que se requiere un certificado de uso válido en el permiso que regula el uso de una clave para cifrado, por ejemplo. De este modo, para utilizar la clave criptográfica, K_{tenant} para cifrado, podría ser necesario presentar un certificado de uso válido para activar el permiso.

[0219] El permiso puede especificar que el certificado de uso debe comprender información a partir de la cual la clave criptográfica K_{tenant} correspondiente al certificado de uso pueda ser identificada para permitir el uso correspondiente al permiso. La ACL puede comprender el *hash* de K_{tenant}.

[0220] La ACL puede comprender una referencia al segundo contexto de seguridad 7. La referencia al segundo contexto de seguridad 7 puede comprender el *hash* de la mitad pública de la clave de identidad $K_{2ID\ pub}$.

[0221] En un modo de realización, el permiso requiere la presentación de un certificado firmado por la mitad privada de una clave asimétrica, $K_{tenant\text{-}sign}$, propiedad del inquilino para permitir el uso asociado al permiso. El permiso especifica que un certificado de uso debe estar firmado por la segunda clave privada $K_{tenant\text{-}signpriv}$ para permitir el uso de la clave criptográfica, K_{tenant}.

[0222] En un modo de realización, el permiso especifica que el certificado de uso debe comprender información a partir de la cual pueda determinarse la expiración del certificado de uso y no debe haber expirado para permitir el uso de la clave criptográfica, K_{tenant} asociado al permiso. Así, el inquilino es capaz de especificar, en el certificado de uso, un tiempo de expiración para su clave, tras el cual la clave no puede ser utilizada hasta que se proporcione otra autorización. Esto permite la transferencia de material criptográfico entre el inquilino y el proveedor de servicios con garantías sobre cuándo puede usarse una clave. Asegura que el uso de la clave solo es posible durante una cantidad de tiempo establecida según sea especificada por el inquilino.

[0223] En un modo de realización, la ACL comprende un permiso que especifica que el certificado de uso debe comprender información a partir de la cual pueda determinarse el "tiempo de inicio" de un periodo de validez del certificado de uso y el tiempo de inicio debe haber transcurrido para permitir el uso de la clave criptográfica, K_{tenant} asociada al permiso. Así, el inquilino es capaz de especificar un periodo de validez de la clave, fuera del cual la clave no puede utilizarse hasta que se proporcione otra autorización. Asegura que el uso de la clave solo es posible durante un intervalo de tiempo establecido según sea especificado por el inquilino

[0224] Para el permiso que regula el almacenamiento de la clave criptográfica, K_{tenant}, la credencial de certificado puede no estar presente. Esto significa que el permiso que regula el almacenamiento está siempre activo, o solo activo hasta que la clave es almacenada en un medio no volátil, por ejemplo. Esto permite que el segundo contexto de seguridad 7 almacene la clave sin un certificado. En el caso de que el permiso que regule el almacenamiento solo esté activo hasta que la clave sea almacenada en un medio no volátil, el permiso es un permiso temporal y se desactiva tras el almacenamiento, es decir, es separado de la ACL.

[0225] El permiso puede especificar que la clave criptográfica, K_{tenant} puede almacenarse fuera del segundo contexto de seguridad 7 solo cuando esté cifrado para su almacenamiento mediante una clave que no puede salir del segundo contexto de seguridad 7. El permiso puede especificar que K_{tenant} solo puede ser cifrada con una clave que no puede salir del segundo contexto de seguridad 7 y no es controlable por el administrador, es decir, el proveedor de servicios. El permiso puede incluir también el mecanismo o mecanismos o tipo o tipo de clave que pueden utilizarse para cifrar la clave de inquilino K_{tenant}, por ejemplo, la clave de inquilino K_{tenant} puede

ser cifrada exclusivamente utilizando cifrado AES-GCM con una clave AES de 256 bits. El permiso puede especificar que la clave criptográfica, K_{tenant} puede también almacenarse dentro del segundo contexto de seguridad 7.

[0226] En un modo de realización, el permiso especifica que la clave criptográfica K_{tenant} y ACL deben ser cifradas con un algoritmo de cifrado autenticado.

[0227] En un modo de realización, el permiso especifica que la información a partir de la cual puede identificarse el origen de la clave criptográfica K_{tenant} es almacenada en la misma estructura de datos que la clave criptográfica K_{tenant} y lista de control de acceso cifradas, y su autenticidad es protegida.

[0228] Alternativamente, el permiso puede especificar que la clave criptográfica, K_{tenant} puede almacenarse exclusivamente dentro del segundo contexto de seguridad 7.

[0229] La ACL de K_{tenant} contiene un permiso que especifica que la clave de inquilino solo puede almacenarse dentro del segundo contexto de seguridad 7 y/o fuera del segundo contexto de seguridad 7 si está cifrada para su almacenamiento fuera del segundo contexto de seguridad 7 por una clave que el proveedor de servicios no puede obtener. Siempre que el segundo contexto de seguridad 7 aplique la política especificada en la ACL, la clave de inquilino K_{tenant} no está expuesta al sistema de proveedor de servicios de alojamiento 3.

[0230] El inquilino ha asegurado que el segundo contexto de seguridad 7 aplicará la política porque ha recibido información que valida que el fabricante del segundo contexto de seguridad 7 es un fabricante de confianza. La información que identifica al fabricante del segundo contexto de seguridad es enviada en el certificado de generación. Por ejemplo, el certificado de generación es firmado con la clave privada de fabricante. Además, el inquilino ha recibido información que valida el producto, *software* y *hardware* del segundo contexto de seguridad 7. Esta información es enviada en el certificado de generación. Dado que el fabricante ha sido identificado como un fabricante de confianza, el inquilino confía en que el segundo contexto de seguridad 7 se ajuste a la información proporcionada por el fabricante. Por ejemplo, si el certificado de generación contiene información que especifica que el *software* y *hardware* es impermeable a ataque por parte del proveedor de servicios, el inquilino confía en que este sea el caso, puesto que la información es proporcionada por el fabricante de confianza. El inquilino puede validar a partir del certificado de generación que el proveedor de servicios está utilizando un segundo contexto de seguridad 7 que tiene determinadas garantías del fabricante. El fabricante puede proporcionar información en el certificado de generación que garantiza que una ACL será aplicada por el segundo contexto de seguridad 7. Puesto que el inquilino confía en el fabricante, también se confía en esta garantía. De este modo, la información de garantía que permite que el inquilino asegure que la ACL será aplicada procede del fabricante. Además, la información de configuración enviada en el certificado de configuración informa al inquilino de si alguien ha intentado manipular el segundo contexto de seguridad 7 bien físicamente o tratando de hackearlo. Una vez que el inquilino confirma que el segundo contexto de seguridad 7 no ha sido manipulado, entonces las garantías del fabricante continúan siendo aplicables.

[0231] La ACL permite la transferencia de material criptográfico entre inquilino y proveedor de servicios, sin exposición del material criptográfico en bruto al proveedor de servicios o a una agencia de seguridad con jurisdicción sobre el proveedor de servicios. Por ejemplo, un inquilino ubicado en Reino Unido no querría que sus claves criptográficas fueran accesibles por un proveedor de servicios estadounidense por miedo a que sus claves sean entregadas a una agencia de seguridad estadounidense que no tenga jurisdicción sobre una empresa ubicada en Reino Unido.

[0232] Además, permite al proveedor de servicios mantener claves de múltiples inquilinos dentro de una sola infraestructura, eliminando la necesidad de mantener un dispositivo específico por inquilino. El inquilino no querría que sus claves fueran accesibles para un tercero, puesto que un tercero que ha sido capaz de extraer una clave del inquilino podría entonces utilizar la clave. Proporcionar la lista de control de acceso que comprende un permiso que especifica que la clave criptográfica, K_{tenant} puede almacenarse exclusivamente dentro del segundo contexto de seguridad 7 y/o fuera del segundo contexto de seguridad 7 si está cifrada para su almacenamiento por una clave que no puede salir del segundo contexto de seguridad 7 permite que múltiples inquilinos utilicen la misma infraestructura criptográfica mientras que se asegura que el material de claves en bruto nunca está expuesto al resto de inquilinos. Los proveedores de servicios e inquilinos son capaces de compartir infraestructura criptográfica de una manera segura para mejorar la eficiencia.

[0233] Un permiso o permisos contenidos en la ACL restringen así cómo puede almacenarse K_{tenant} y se establecen de manera que K_{tenant} sea inaccesible para cualquiera incluyendo el proveedor de servicios. Dado que un permiso correspondiente a un primer tipo de uso de la clave solo puede activarse por una credencial de certificado firmada por una clave privada conocida solo por el inquilino, el segundo contexto de seguridad 7 rechazará el primer tipo de uso de la clave hasta que se presente un certificado de autorización con la clave. Esto significa que el primer tipo de uso del material de clave en bruto no es accesible para ningún tercero incluyendo al proveedor de servicios. De este modo, el inquilino es capaz de mantener la garantía de que sus claves criptográficas no son expuestas al proveedor de servicios o cualquier otra parte. El inquilino es capaz de controlar el uso de su clave una vez sea importada al segundo contexto de seguridad a través de la lista de control de acceso.

[0234] La lista de control de acceso puede especificar que deba proporcionarse información concreta en el certificado de uso para permitir determinados usos de la clave de inquilino K_{tenant}. De este modo, el inquilino puede restringir cómo es utilizada la clave por el proveedor de servicios. Por ejemplo, la ACL puede contener un permiso que especifique que la clave de inquilino puede utilizarse para cifrar datos cuando se presenta un certificado firmado con una clave privada determinada. De este modo, la credencial asociada al permiso es el certificado firmado con la clave privada determinada. También puede incluir un permiso que especifique que el descifrado está disponible cuando se presente mediante un certificado firmado por una clave privada diferente. Cada permiso puede requerir una credencial diferente, por ejemplo, un certificado firmado por una clave privada diferente.

[0235] La información adicional que un permiso puede especificar está contenida en el certificado puede incluir la hora en la que fue emitido el certificado, donde el sello de tiempo comprende una referencia a un reloj de confianza compartido y/o la identidad (por ejemplo, el *hash* de K_{IDpub}) del dispositivo con el que puede utilizarse el certificado. Incluir la identidad limita los dispositivos dentro de un contexto con los que puede utilizarse una clave.

[0236] La confianza establecida con el segundo contexto de seguridad y la provisión de la ACL correspondiente a la clave de inquilino K_{tenant} permite al inquilino validar criptográficamente que un proveedor de servicios se adhiere a un conjunto de normas, es decir, aquellas proporcionadas en la ACL, que garantiza la no divulgación de material criptográfico en bruto y uso una vez que la clave ha sido transferida. Permite que el inquilino conceda de manera segura y verificable claves criptográficas al proveedor de servicios para su uso de una manera restringida, a la vez que se soporta la multitenencia.

[0237] La ACL comprende políticas que aseguran que el proveedor de servicios no tiene acceso al material de claves en bruto de un inquilino, el inquilino tiene la garantía de que su clave solo puede ser utilizada en situaciones bajo su control, y múltiples inquilinos pueden compartir la misma infraestructura criptográfica de una manera segura. Permite conceder la clave K_{tenant} al tiempo que se limita el periodo de tiempo en el que puede ser utilizada. Permite a los inquilinos controlar de manera precisa el uso de sus claves una vez que son alojadas por un proveedor de servicios.

[0238] Tras la generación de K_{tenant}, el inquilino inicia entonces un protocolo de préstamo de clave con el proveedor de servicios. Por ejemplo, el primer contexto de seguridad 5 puede enviar un mensaje al segundo contexto de seguridad 7 que inicia el paso S602. El mensaje puede solicitar $K_{BLOB\ pub}$.

[0239] En el paso S602, un primer par de claves criptográficas que es adecuado para su uso en el esquema de cifrado y un primer certificado criptográfico C_{BLOB} son generados en el segundo contexto de seguridad 7, comprendiendo el primer par de claves criptográficas una primera clave pública, $K_{BLOB\ pub}$, y una primera clave privada, $K_{BLOB\ priv}$. En un modo de realización, el primer certificado criptográfico comprende un *hash* de la primera clave pública, $K_{BLOB\ pub}$.

[0240] En un modo de realización, un nuevo primer par de claves criptográficas K_{BLOB} y primer certificado criptográfico C_{BLOB} son generados para cada transferencia de datos, en otras palabras, cada primer par de claves criptográficas K_{BLOB} y primer certificado criptográfico C_{BLOB} es válido exclusivamente para un solo uso.

[0241] En un modo de realización, el primer certificado criptográfico C_{BLOB} y el certificado de configuración son un solo certificado. En otras palabras, en lugar del método de la figura 2(b), el primer certificado criptográfico es generado comprendiendo además información relativa a la configuración actual del segundo contexto de

seguridad. La información relativa a la configuración actual del segundo contexto de seguridad puede ser la descrita en relación con la figura 2(b).

[0242] En el paso S603, el primer certificado criptográfico C_{BLOB} es firmado criptográficamente con la mitad privada de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ priv}$. El segundo procesador 19 está configurado para firmar criptográficamente el primer certificado criptográfico C_{BLOB} con la mitad privada de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ priv}$.

[0243] En un modo de realización, el primer certificado criptográfico C_{BLOB} valida que $K_{BLOB\ pub}$ fue generado en el segundo contexto de seguridad 7. El primer certificado criptográfico comprende información a partir de la cual puede validarse el origen de la clave criptográfica $K_{BLOB\ pub}$. En un modo de realización, la información a partir de la cual el origen de la clave criptográfica $K_{BLOB\ pub}$ puede validarse es el *hash* firmado de la primera clave pública, $K_{BLOB\ pub}$. En otras palabras, el primer certificado criptográfico C_{BLOB} comprende un *hash* de la primera clave pública $K_{BLOB\ pub}$ y es firmado con la mitad privada de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ priv}$, que permite que se valide el origen de la primera clave pública, $K_{BLOB\ pub}$.

[0244] El primer certificado criptográfico es firmado por $K_{2ID\ priv}$ para probar que el proveedor de servicios generó el certificado. Incluir el *hash* también valida que los datos, es decir, la primera clave pública, $K_{BLOB\ pub}$ no ha sido manipulada durante el tránsito.

[0245] En un modo de realización, el primer certificado criptográfico comprende información que valida que $K_{BLOB\ priv}$ es efímero y que $K_{BLOB\ priv}$ no puede salir del segundo contexto de seguridad. La información que indica que $K_{BLOB\ priv}$ es efímera y que $K_{BLOB\ priv}$ no puede salir del segundo contexto de seguridad es enviada con el primer par de claves criptográficas K_{BLOB} al primer contexto de seguridad 5. El primer certificado criptográfico comprende esta información y es firmado, validando así la información contenida en el mensaje.

[0246] En el paso S604, la primera clave pública, $K_{BLOB,}$ y el primer certificado criptográfico firmado $\{C_{BLOB}\}_{K2ID\ priv}$ son enviados al primer contexto de seguridad 5. La información relativa a $K_{BLOB\ pub}$, por ejemplo, indicando que $K_{BLOB\ priv}$ es efímero y que $K_{BLOB\ priv}$ no puede salir del segundo contexto de seguridad, puede también enviarse con el primer par de claves criptográficas K_{BLOB} al primer contexto de seguridad 5 y estar incluida en el primer certificado. El segundo transceptor 15 está configurado para enviar la primera clave pública, $K_{BLOB\ pub}$, y el primer certificado criptográfico firmado $\{C_{BLOB}\}_{K2ID\ priv}$ al primer contexto de seguridad 5. La información de configuración y/o información sobre la clave puede enviarse al primer contexto de seguridad 5 en el mismo mensaje.

[0247] De este modo, en los pasos del S602 al S604, el segundo contexto de seguridad 7, en respuesta al mensaje de iniciación, genera una clave asimétrica, K_{BLOB}, y envía la mitad pública y un certificado firmado por la mitad privada de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ priv}$ al primer contexto de seguridad 5. K_{BLOB} es una clave asimétrica efímera, generada dentro del segundo contexto de seguridad 7 con un certificado de clave que acompaña, C_{BLOB}. C_{BLOB} permite al inquilino validar que la clave fue generada por un dispositivo dentro del segundo contexto de seguridad 7, que la mitad privada de K_{blob} es efímera y no puede salir nunca del segundo contexto de seguridad 7. El proveedor de servicios envía la mitad pública de K_{BLOB} y C_{BLOB} al primer contexto de seguridad 5.

[0248] En el paso S605, el primer certificado criptográfico firmado $\{C_{BLOB}\}_{K2ID\ priv}$ es verificado en el primer contexto de seguridad 5. El primer procesador 17 en el primer contexto de seguridad 5 es configurado para verificar el primer certificado criptográfico firmado $\{C_{BLOB}\}_{K2ID\ priv}$. El primer certificado criptográfico firmado $\{C_{BLOB}\}_{K2ID\ priv}$ es verificado utilizando la mitad pública de la clave de identidad del segundo contexto de seguridad, $K_{2ID\ pub}$. El primer procesador 17 es configurado para llevar a cabo un algoritmo de verificación de firma que, dado el mensaje firmado $\{C_{BLOB}\}_{K2ID\ priv}$ y la clave pública $K_{2ID\ pub}$ acepte o rechace la declaración de autenticidad del mensaje.

[0249] La autenticidad de la primera clave pública, $K_{BLOB\ pub}$ es validada entonces en el primer contexto de seguridad 5 a partir del primer certificado criptográfico C_{BLOB}. El primer procesador 17 en el primer contexto de seguridad 5 es configurado para validar la primera clave pública, $K_{BLOB\ pub}$. En un modo de realización en el que el primer certificado criptográfico C_{BLOB} comprende un *hash* de la primera clave pública, $K_{BLOB\ pub}$, la autenticidad de la primera clave pública, $K_{BLOB\ pub}$ es validada calculando el *hash* de la primera clave pública, $K_{BLOB\ pub}$, y validando que se corresponde con el contenido en el primer certificado criptográfico C_{BLOB}. Cualquier otra

información enviada con la primera clave pública, $K_{BLOB\ pub}$, por ejemplo, información de configuración actual e información en relación con la primera clave pública, $K_{BLOB\ pub}$, también es validada a partir del certificado.

[0250] Si la firma es verificada, la primera clave pública, $K_{BLOB\ pub}$, es almacenada en la primera memoria de dispositivo 9 del primer contexto de seguridad 5. Alternativamente, puede protegerse su integridad por el primer contexto de seguridad 5 y almacenarse en un almacenamiento no de confianza fuera del primer contexto de seguridad 5.

[0251] Si la firma no es verificada o la clave no es validada, se devuelve un error al segundo contexto de seguridad 7, por ejemplo, se envía un mensaje indicando "Acceso denegado". En este momento, se termina la comunicación entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7.

[0252] En un modo de realización en el que el primer certificado criptográfico C_{BLOB} es generado comprendiendo además información en relación con la configuración actual del segundo contexto de seguridad, la información relativa a la configuración actual del segundo contexto de seguridad también es validada en el paso S605, como se describe en relación con la figura 2(b). Cualquier información de clave incluida en el mensaje también es validada.

[0253] De este modo, en el paso S605, el primer contexto de seguridad puede utilizar el certificado para validar los parámetros de K_{BLOB}, autenticar la fuente y comprobar que está bien formada y se ajusta a las políticas de seguridad esperadas por el inquilino. La política de seguridad que un inquilino puede requerir podría incluir una longitud de clave, tipo de clave y/o pares de credencial-permiso de clave. Los permisos de clave se utilizan para describir las operaciones para las que puede utilizarse una clave. Por ejemplo, los permisos pueden especificar que una clave puede utilizarse para cifrar otras claves o que puede utilizarse para firmar datos criptográficamente. Los permisos deben activarse mediante una credencial correspondiente antes de poder utilizarse. Una credencial en este sistema toma la forma de un certificado criptográfico verificable. El primer contexto de seguridad 5 valida C_{BLOB}, que la mitad privada de K_{BLOB} es efímera, que el segundo contexto de seguridad 7 es fabricado por una fuente de confianza y que el estado del segundo contexto de seguridad 7 es adecuado para prestarle una clave.

[0254] El paso S606 comprende cifrar la clave criptográfica K_{tenant} y la lista de control de acceso correspondiente con la primera clave pública $K_{BLOB\ pub}$ en el primer contexto de seguridad 5. El primer procesador 17 es configurado para cifrar la clave criptográfica K_{tenant} y la lista de control de acceso correspondiente con la primera clave pública $K_{BLOB\ pub}$.

[0255] Puesto que el canal de comunicación entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7 es proporcionado y controlado por el proveedor de servicios, no resulta de confianza para el inquilino para la transferencia de claves criptográficas de alto valor como K_{tenant}, puesto que podría estar abierto a ataques por parte del proveedor de servicios. De este modo, la seguridad de K_{tenant} es aplicada por el inquilino mediante el cifrado de K_{tenant} con la primera clave pública $K_{BLOB\ pub}$. El primer certificado C_{BLOB} permite que el inquilino valide que la mitad privada de K_{blob} no puede salir nunca del segundo contexto de seguridad 7, así mediante cifrado de K_{tenant} con la primera clave pública $K_{BLOB\ pub}$, el inquilino puede garantizar que K_{tenant} está segura frente al proveedor de servicios, aunque el proveedor de servicios pueda atacar el canal de comunicación.

[0256] El cifrado de la clave de inquilino proporciona de este modo un canal seguro que se basa en la confianza entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7. Esto permite un canal autenticado de seguridad de nivel superior que no es de confianza para el primer contexto de seguridad 5 y el segundo contexto de seguridad 7 a utilizar entre el inquilino y el sitio del proveedor de servicios. Este canal seguro de capa superior puede proporcionarse por el proveedor de servicios utilizando un balanceador de carga o cortafuegos. El cifrado de la clave de inquilino permite al proveedor de servicios continuar utilizando esta infraestructura para mitigar ataques como denegación del servicio al tiempo que permite la seguridad de contexto a contexto sin tener que confiar en servicios de seguridad externos.

[0257] $K_{BLOB\ pub}$ puede ser descartada por el inquilino tras el cifrado de K_{tenant}.

[0258] En un modo de realización, la información a partir de la cual el origen de la clave criptográfica K_{tenant} puede ser validado es la clave de inquilino y lista de control de acceso cifradas firmadas $\{\{K_{tenant}, ACL\}\ K_{BLOB\ pub}\}\ K_{tenant\text{-}sign\ priv}$.

[0259] De este modo, en el paso S607, el blob de salida del paso S606 es firmado criptográficamente utilizando la mitad privada de $K_{tenant\text{-}sign}$. El primer procesador 17 es configurado para firmar criptográficamente el blob de salida del paso S606 con la mitad privada de $K_{tenant\text{-}sign}$.

[0260] En el paso S608, se envía la clave criptográfica y lista de control de acceso correspondiente cifradas {K_{tenant}, ACL} $K_{BLOB\ pub}$, e información a partir de la cual el origen de la clave criptográfica K_{tenant} puede validarse, al segundo contexto de seguridad 7. En un modo de realización, también se envía información a partir de la cual puede identificarse el origen del mensaje, que puede ser el *hash* de la mitad pública de $K_{tenant\text{-}sign}$, por ejemplo.

[0261] En un modo de realización, en el que la información a partir de la cual puede identificarse el origen del mensaje comprende un *hash* de $K_{tenant\text{-}signpub}$, el blob cifrado, *hash* de la clave de firma y firma son enviados al segundo contexto de seguridad 7. La firma es información a partir de la cual puede validarse el origen de la clave criptográfica K_{tenant}. El primer transceptor 13 es configurado para enviar el blob cifrado, blob de salida firmado del paso S607 y el *hash* de la mitad pública de $K_{tenant\text{-}sign}$ al segundo contexto de seguridad 7.

[0262] Dada una clave aceptable $K_{BLOB\ pub}$, que es una clave $K_{BLOB\ pub}$ que el inquilino define como de suficiente fuerza criptográfica, la clave que se va a registrar, K_{tenant}, es cifrada con la mitad pública de K_{blob} en el primer contexto de seguridad 5. Como se ha descrito anteriormente, K_{tenant} incluye pares de credencial-permiso, es decir, la ACL, que especifica las operaciones aceptables para las cuales puede utilizarse el material de claves y que pueden ser activadas mediante un certificado que debe estar firmado por la mitad privada de $K_{tenant\text{-}sign}$. El blob cifrado es firmado utilizando la mitad privada de $K_{tenant\text{-}sign}$ y el blob cifrado, firma y *hash* de la mitad pública de $K_{tenant\text{-}sign}$ son enviados al segundo contexto de seguridad 7.

[0263] La transferencia de la clave criptográfica K_{tenant} al segundo contexto de seguridad en el proveedor de servicios está protegida frente al proveedor de servicios y otros atacantes, ya que la clave utilizada para cifrar la clave criptográfica K_{tenant} no es recuperable en texto no cifrado. Se requiere que $K_{blobpriv}$ descifre con éxito los datos enviados desde el primer contexto de seguridad 5 al segundo contexto de seguridad 7. $K_{blobpriv}$ es efímero y no puede ser accedido o mutado por el proveedor de servicios o un tercero.

[0264] La figura 6(b) es un diagrama de flujo que muestra etapas adicionales de un método de transferencia de una clave criptográfica, K_{tenant} del primer contexto de seguridad 5 al segundo contexto de seguridad 7 según un modo de realización de la presente invención.

[0265] En el paso S609, el origen de la clave criptográfica K_{tenant} es validado en el segundo contexto de seguridad 7. En un modo de realización, esto es validado verificando en primer lugar la firma contenida en el mensaje enviado desde el primer contexto de seguridad 5.

[0266] En un modo de realización, el *hash* de la mitad pública de $K_{tenant\text{-}sign}$ es utilizado para identificar al inquilino del cual procede el mensaje, e identificar así la clave de firma correcta requerida para verificar la firma.

[0267] A continuación se verifica la firma utilizando la mitad pública de $K_{tenant\text{-}sign}$. El segundo procesador 19 en el segundo contexto de seguridad 7 es configurado para verificar la firma. La firma se verifica utilizando la mitad pública de $K_{tenant\text{-}sign}$. El segundo procesador 19 es configurado para llevar a cabo un algoritmo de verificación de firma que, dada la firma y la clave pública $K_{tenant\text{-}sign}$ acepte o rechace la declaración de autenticidad del mensaje.

[0268] A continuación, se valida que el contenido de la firma se corresponde con el del blob cifrado. Esto permite la validación del origen del blob cifrado.

[0269] Si se verifica y valida, el método avanza al paso S610. Si no se verifica o valida, se devuelve un error al primer contexto de seguridad 5, por ejemplo, se envía un mensaje indicando "Acceso denegado". En este momento, se termina la comunicación entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7.

[0270] El paso S610 comprende descifrar la clave criptográfica K_{tenant} y lista de control de acceso correspondiente cifradas con la primera clave privada $K_{BLOB\ priv}$ en el segundo contexto de seguridad 7. El segundo procesador 19 es configurado para descifrar la clave criptográfica, K_{tenant}, y lista de control de acceso correspondiente cifradas. El segundo procesador 19 es configurado para llevar a cabo un algoritmo de descifrado

dada la clave criptográfica K_{tenant} y la lista de control de acceso correspondiente cifradas y la primera clave privada $K_{BLOB\ priv}$.

[0271] El paso S611 comprende recifrar la clave criptográfica K_{tenant} y la ACL con una tercera clave criptográfica en el segundo contexto de seguridad 7. Este paso es llevado a cabo de manera que la clave criptográfica K_{tenant} y la ACL puedan ser almacenadas fuera del segundo contexto de seguridad 7. En un modo de realización alternativo, este paso es omitido y la clave criptográfica Ktenant, la ACL e información que identifica el origen de la clave criptográfica Ktenant son almacenadas sin cifrar en el segundo contexto de seguridad 7.

[0272] La ACL especifica los parámetros de qué tipo o tipos de clave pueden utilizarse para cifrar K_{tenant}, y qué mecanismos de cifrado pueden ser utilizados.

[0273] La ACL puede comprender un permiso, es decir, una política, que establece que K_{tenant} solo puede ser cifrada por una clave que no puede salir del segundo contexto de seguridad 7 y no es controlable por el administrador, es decir, el proveedor de servicios. El permiso incluye también el mecanismo o mecanismos o tipo o tipo de clave que pueden utilizarse para cifrar la clave de inquilino K_{tenant}, por ejemplo, la clave de inquilino K_{tenant} puede ser cifrada exclusivamente utilizando cifrado AES-GCM (Galois/Counter Mode) con una clave AES de 256 bits.

[0274] El mecanismo de cifrado puede especificar la necesidad de asegurar la autenticidad, integridad y confidencialidad o algún subconjunto de aquellas propiedades.

[0275] El segundo contexto de seguridad 7 puede reutilizar una clave existente que cumple los requisitos de la política de ACL, o crear una nueva clave.

[0276] La clave criptográfica K_{tenant} y la ACL son cifradas en el segundo contexto de seguridad 7 utilizando el mecanismo especificado, y una tercera clave criptográfica que cumple los requisitos especificados. El segundo procesador es configurado para cifrar la clave criptográfica K_{tenant} con una tercera clave criptográfica. En un modo de realización, la clave criptográfica, K_{tenant} es cifrada para su almacenamiento por una clave que no puede salir del segundo contexto de seguridad 7.

[0277] La clave criptográfica K_{tenant} y la ACL pueden cifrarse utilizando un algoritmo de cifrado autenticado.

[0278] En un modo de realización, la clave criptográfica K_{tenant} y ACL son entradas para ser cifradas en un algoritmo de cifrado autenticado, por ejemplo, una operación AES-GCM, mientras que la información a partir de la cual puede identificarse el origen de la clave criptográfica K_{tenant} es entrada como un parámetro de datos autenticado. En un modo de realización, la información a partir de la cual el origen de la clave criptográfica K_{tenant} puede identificarse es la mitad pública de $K_{tenant\text{-}sign}$. En un modo de realización, un *hash* de K_{tenant} es almacenado también con la clave criptográfica K_{tenant}, por ejemplo, el *hash* de k_{tenant} puede ser el nombre del archivo en el que los datos cifrados son almacenados.

[0279] La clave criptográfica K_{tenant} y lista de control de acceso correspondiente recifradas y la información autenticada a partir de la cual puede identificarse el origen de la clave criptográfica K_{tenant}, son transferidas a una memoria de dispositivo fuera del segundo contexto de seguridad 7.

[0280] La información a partir de la cual puede identificarse el origen de la clave criptográfica K_{tenant} es almacenada así en la misma estructura de datos que la clave criptográfica K_{tenant} y lista de control de acceso cifradas, pero no es necesariamente cifrada. Sin embargo, se protege la autenticidad de la información a partir de la cual puede identificarse el origen de la clave criptográfica K_{tenant}, de manera que no pueda ser cambiada sin aviso.

[0281] En los pasos descritos anteriormente, tras su recepción, el segundo contexto de seguridad 7 verifica la firma de carga útil utilizando la mitad pública de $K_{tenant\text{-}sign}$. El *hash* contenido en la carga útil recibida es utilizado para identificar la mitad pública de la clave de firma del inquilino. La firma de carga útil recibida es verificada utilizando la clave de firma identificada. Tras la correcta validación de la carga útil, K_{tenant} es descifrada utilizando la mitad privada de K_{blob} y recifrada bajo una clave no recuperable, según imponga la ACL de K_{tenant}, y almacenada junto con la mitad pública de $K_{tenant\text{-}sign}$ fuera del segundo contexto de seguridad 7 para su uso

posterior. Alternativamente, la clave K_{tenant} es almacenada sin cifrar en memoria no volátil protegida dentro del segundo contexto de seguridad 7. En ambos casos, la clave descifrada es almacenada así de manera segura y a prueba de manipulaciones.

[0282] La manera en la que K_{tenant} se almacena es descrita por sus permisos o políticas. De manera específica, en el momento de la generación, los permisos concedidos restringen cómo K_{tenant} puede ser almacenada y se establecen de manera que K_{tenant} sea inaccesible para cualquiera, incluyendo el proveedor de servicios, que no sea el segundo contexto de seguridad 7.

[0283] En un modo de realización en el que una pluralidad de inquilinos almacena una clave con un solo proveedor de servicios, cada una de las claves de inquilino puede ser cifrada para su almacenamiento con la misma clave. De manera alternativa, cada clave de inquilino puede cifrarse con una clave diferente si existen diferentes permisos de almacenamiento entre las ACL correspondientes a cada clave de inquilino, por ejemplo.

[0284] La figura 7(a) es una ilustración esquemática de un método de inscripción de clave, que es parte de un método de transferencia de claves criptográficas según un modo de realización de la presente invención. El método comprende los pasos de S602 a S611 descritos en relación con las figuras 6(a) y (b) anteriormente.

[0285] Se envía un mensaje de inscripción de clave desde el primer contexto de seguridad 5 al segundo contexto de seguridad 7. En respuesta a este mensaje, el primer par de claves criptográficas K_{BLOB} es generado en el segundo contexto de seguridad 7. El segundo contexto de seguridad 7 envía la mitad pública del primer par de claves criptográficas K_{BLOB} y el primer certificado criptográfico firmado $\{C_{BLOB}\}_{K2ID\ priv}$ al primer contexto de seguridad 5, donde son validados. La clave criptográfica K_{tenant} es cifrada en el primer contexto de seguridad 5 con $K_{BLOB\ pub}$. La clave cifrada $\{K_{tenant}\}_{KBLOB\ pub}$ y *hash* $\{K_{tenant\text{-}sign\ pub}\}$ son firmados con $K_{tenant\text{-}sign\ priv}$ en el primer contexto de seguridad 5. El mensaje firmado es enviado al segundo contexto de seguridad 7 donde es validado y la clave cifrada $\{K_{tenant}\}_{KBLOB\ pub}$ es descifrada y recifrada en el segundo contexto de seguridad 7 con una clave no recuperable que está a salvo del administrador. A continuación, la clave de inquilino cifrada puede ser almacenada fuera del segundo contexto de seguridad 7.

[0286] La figura 7(b) es un diagrama de flujo de un método de transferencia de claves criptográficas según un modo de realización de la presente invención.

[0287] El inquilino establece la ACL de la clave de inquilino en el primer contexto de seguridad 5. A continuación, el primer contexto de seguridad 5 solicita la primera clave pública $K_{BLOB\ pub}$ del segundo contexto de seguridad 7. El primer contexto de seguridad 5 envía un mensaje de solicitud al segundo contexto de seguridad 7, por ejemplo. A continuación, el primer contexto de seguridad 5 valida la primera clave pública recibida $K_{BLOB\ pub}$ y primer certificado criptográfico C_{BLOB}. Esto corresponde al paso S605 descrito anteriormente. Si la primera clave pública $K_{BLOB\ pub}$ y el primer certificado criptográfico C_{BLOB} no son validados, se devuelve un error. Si son validados, el primer contexto de seguridad 5 cifra la clave de inquilino y ACL asociada con la primera clave pública $K_{BLOB\ pub}$. Esto corresponde al paso S606 descrito anteriormente. A continuación, el primer contexto de seguridad 5 firma la clave y ACL asociada cifradas y un *hash* de $K_{tenant\text{-}sign\ pub}$ con $K_{tenant\text{-}sign\ priv}$. Esto corresponde al paso S607 descrito anteriormente. A continuación, el primer contexto de seguridad 5 intercambia el blob cifrado, el *hash* de $K_{tenant\text{-}sign\ pub}$ y la firma con el segundo contexto de seguridad 7. Esto corresponde al paso S608 descrito anteriormente.

[0288] La figura 8(a) es una ilustración esquemática del sistema de inquilino 1 y del sistema de proveedor de servicios 3 después de que la clave de inquilino K_{tenant} haya sido importada al segundo contexto de seguridad 7. En un modo de realización, K_{blob} y C_{blob} son transitorios, y una vez que K_{tenant} ha sido transferida, son eliminados del segundo contexto de seguridad 7 y el primer contexto de seguridad 5.

[0289] La primera memoria de dispositivo 9 en el primer contexto de seguridad 5 también almacena la primera clave pública $K_{BLOB\ pub}$. Alternativamente, esta clave puede almacenarse fuera del primer contexto de seguridad 5 de manera que se proteja su integridad. La segunda memoria de dispositivo 11 en el segundo contexto de seguridad 7 también almacena la clave de inquilino K_{tenant} y la ACL correspondiente. Alternativamente, la clave de inquilino K_{tenant} y ACL pueden almacenarse fuera del segundo contexto de seguridad 7, cifradas con una tercera clave criptográfica que no puede salir del segundo contexto de seguridad 7.

[0290] La figura 8(b) es una ilustración esquemática de una fuente de tiempo de referencia segura y a prueba de manipulaciones 2, que puede ser alojada por el proveedor de servicios, el inquilino o un tercero independiente. Si es alojada por el proveedor de servicios, la fuente de tiempo de referencia puede ser parte del segundo contexto de seguridad 7, o puede ser un contexto de seguridad diferente.

[0291] La fuente de tiempo 2 comprende una tercera memoria de dispositivo 35. La tercera memoria de dispositivo 35 está configurada para almacenar información criptográfica como claves, pares de claves y certificados. La tercera memoria de dispositivo 35 puede incluir cualquier forma de memoria de dispositivo no volátil como *flash*, discos ópticos o discos duros magnéticos, por ejemplo. La fuente de tiempo 2 también comprende memoria volátil.

[0292] La tercera memoria de dispositivo 35 almacena una clave de identidad asimétrica única K_{TSID}, con un certificado de generación firmado correspondiente $\{C_{TSID}\}_{Kman\ priv}$. K_{TSID} es una clave de firma utilizada para probar el origen de los datos y autenticidad. El certificado de generación C_{TSID} puede describir los parámetros públicos de la clave, por ejemplo, información relativa al tipo de la clave y su longitud. El certificado de generación C_{TSID} comprende información que autentica que la clave de identidad K_{TSID} fue generada en una fuente de tiempo 2. Por ejemplo, el certificado de generación C_{TSID} puede comprender el *hash* firmado de la mitad pública de K_{TSID}. El certificado de generación C_{TSID} puede incluir también información de estado, por ejemplo, información relativa a una identificación única del dispositivo, información que identifica al fabricante, la versión de dispositivo, la versión de *hardware*, el tipo de *software* y las características del modelo soportadas. El certificado de generación C_{TSID} es firmado por un fabricante de confianza tanto para el primer contexto de seguridad 5 como para el segundo contexto de seguridad 7. El certificado de generación es firmado criptográficamente con la mitad privada de una clave asimétrica de fabricante, $K_{man\ priv}$. El fabricante puede ser un tercero que fabricó el dispositivo o dispositivos de seguridad que forman el primer contexto de seguridad, el dispositivo o dispositivos de seguridad que forman el segundo contexto de seguridad y la fuente de tiempo 2.

[0293] La fuente de tiempo 2 comprende además un tercer transceptor 39. El tercer transceptor 39 está configurado para transmitir y recibir paquetes de datos. Los paquetes de datos pueden ser transmitidos desde y recibidos en el transceptor 39 a través de una conexión a internet inalámbrica, por ejemplo.

[0294] La fuente de tiempo 2 comprende además un tercer procesador 41. El tercer procesador 41 es configurado para llevar a cabo operaciones criptográficas, como generación de claves criptográficas y pares de claves criptográficas asimétricos, generación de certificados correspondientes a una clave criptográfica o par de claves criptográficas asimétrico, generación de listas de control de acceso correspondientes a una clave criptográfica, generación de certificados de uso correspondientes a una clave criptográfica, cifrado de un objeto con una clave criptográfica que es almacenada en la tercera memoria de dispositivo 35, descifrado de un objeto cifrado con una clave criptográfica que es almacenada en la tercera memoria de dispositivo 35, firmar criptográficamente un objeto con una clave criptográfica que es almacenada en la tercera memoria del dispositivo 35, verificación de una firma y validación de un objeto basándose en información almacenada en la tercera memoria del dispositivo 35.

[0295] La fuente de tiempo 2 comprende además un reloj 37. El reloj 37 puede ser un reloj monotónico, es decir, un contador que aumenta monotónicamente con el tiempo. El reloj puede representar la hora del día con un alto grado de precisión. En un modo de realización, el reloj tiene una precisión de 1 segundo o mejor. Por ejemplo, el reloj puede basarse en una señal GPS que tiene una precisión del orden de 40 nanosegundos.

[0296] La fuente de tiempo 2 puede ser resistente frente a manipulaciones, por ejemplo, mediante la inclusión de seguridad física como una membrana que cubre el dispositivo entero, que no puede ser eliminada sin destruir el *hardware* físico subyacente, haciéndolo así inutilizable.

[0297] Los tres servicios mostrados en la figura 8(a) y 8(b) comprendiendo: 1) el primer contexto de seguridad 5, por ejemplo, un dispositivo de seguridad, propiedad del inquilino y operado por este; 2) el segundo contexto de seguridad 7, por ejemplo, uno o más dispositivos de seguridad propiedad del proveedor de servicios y operados por este; y 3) una fuente de tiempo de confianza 2, que puede ser propiedad del proveedor de servicios, un tercero externo o un inquilino, son un conjunto de servicios de cooperación que pueden verificar todos que están construidos por terceros de confianza con un conjunto de propiedades de seguridad conocidas y adherirse a determinadas normas iguales. Se presupone que un inquilino confía en los terceros antes mencionados que han construido los servicios de cooperación, pero no confía en el proveedor de servicios que aloja algunos de estos servicios. Un contexto de seguridad puede ser uno o más dispositivos de seguridad que comparten un

conjunto de primitivas criptográficas y forman un clúster a través del cual puede realizarse un balanceo de carga de las solicitudes.

[0298] Cada uno del primer contexto de seguridad 5, segundo contexto de seguridad 7 y fuente de tiempo de referencia 2 puede identificarse de manera verificable utilizando un certificado criptográfico, que puede generarse en el momento de la fabricación, por ejemplo. Cada uno es capaz de almacenar de manera segura su identidad de una manera que significa que no pueden ser imitados. Identificar el primer contexto de seguridad 5, segundo contexto de seguridad 7 o fuente de tiempo de referencia 2 permite que su origen pueda ser comprobado.

[0299] Además, la configuración y estado de cada uno del primer contexto de seguridad 5, segundo contexto de seguridad 7 y fuente de tiempo de referencie 2 pueden validarse de una manera no rechazable. El origen y el estado de un servicio define información suficiente por la que otros servicios pueden depositar su confianza.

[0300] Cada componente contiene una K_{ID} generada en la fábrica cuando fue fabricado, por ejemplo. Cada componente contiene también el certificado de clave para la K_{ID} que es firmado utilizando una clave asimétrica conocida solo por el fabricante. La mitad pública de la clave de fabricante puede utilizarse como la raíz de confianza para autenticar los dispositivos auténticos.

[0301] La transferencia de certificados criptográficos y claves criptográficas entre la fuente de tiempo de referencia 2 y el segundo contexto de seguridad 7 descrito a continuación puede tener lugar a través de un canal seguro autenticado entre la fuente de tiempo de referencia 2 y el segundo contexto de seguridad 7, que es proporcionado y controlado por el proveedor de servicios. Cabe observar que aunque el canal pueda estar protegido frente a terceros, está abierto a ataques por parte del proveedor de servicio, y por tanto no es de confianza.

[0302] El intercambio de claves públicas y certificados descrito en relación con la figura 9 a continuación permite que se establezca una relación de confianza entre el segundo contexto de seguridad 7 y la fuente de tiempo 2.

[0303] La figura 9 es un diagrama de flujo que muestra un método de registro de una fuente de tiempo 2 con el segundo contexto de seguridad 7. Este puede llevarse a cabo en cualquier momento como parte del método de transferencia de claves según un modo de realización de la presente invención, o como parte del método de control del uso de una clave criptográfica según un modo de realización de la presente invención. Por ejemplo, el método de registrar una fuente de tiempo 2 puede llevarse a cabo cuando el administrador del segundo contexto de seguridad 7 establece los dispositivos en el segundo contexto de seguridad 7, es decir, cuando se desarrolla la autenticidad. Esto es un proceso no frecuente y puede ser necesario llevarlo a cabo solo una vez. Tras la inscripción de la fuente de tiempo 2, el segundo contexto de seguridad 7 puede entonces transmitir información relativa a sus fuentes de tiempo de confianza a inquilinos potenciales. Por tanto, los inquilinos saben inicialmente qué fuente o fuentes de tiempo soporta el proveedor de servicios y pueden tomar decisiones acerca de si estas fuentes de tiempo son aceptables antes de que comience la inscripción de claves, por ejemplo, validando la autenticidad, el estado y configuración de la fuente o fuentes de tiempo como se describe en relación con la figura 10 a continuación.

[0304] Si la fuente de tiempo de referencia 2 es parte del segundo contexto de seguridad 7, no es necesario registrar la fuente de tiempo 2 con el segundo contexto de seguridad 7 y estos pasos no pueden llevarse a cabo.

[0305] Una fuente de tiempo de referencia 2 comprende una memoria de dispositivo 35 y un reloj 37 como se ha descrito anteriormente en relación con la figura 8(b).

[0306] En el paso S901, la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$, y el certificado de generación $\{C_{TSID}\}_{Kman\ priv}$, son enviados desde la fuente de tiempo de referencia 2 al segundo contexto de seguridad 7 en respuesta a un mensaje de consulta del segundo contexto de seguridad 7. Un transceptor 39 en la fuente de tiempo de referencia 2 es configurado para enviar la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$, y el certificado de generación $\{C_{TSID}\}_{Kman\ priv}$, al segundo transceptor 15 en el segundo contexto de seguridad 7. La información relativa al estado del dispositivo de fuente de tiempo 2 puede enviarse en el mismo mensaje. La información relativa al estado del dispositivo también estará contenida en el certificado de generación en este caso, para permitir la validación de la información de estado.

[0307] En el paso S902, el certificado de generación $\{C_{TSID}\}_{Kman\ priv}$ es verificado en el segundo contexto de seguridad 7. El segundo procesador 19 en el segundo contexto de seguridad 7 es configurado para verificar el certificado de generación $\{C_{TSID}\}_{Kman\ priv}$. El certificado de generación es verificado utilizando la mitad pública de la clave de fabricante de confianza $K_{man\ pub}$. El segundo procesador 19 es configurado para llevar a cabo un algoritmo de verificación de firma que, dado el mensado firmado $\{C_{TSID}\}_{Kman\ priv}$ y la clave pública $K_{man\ pub}$ acepte o rechace la declaración de autenticidad del mensaje.

[0308] La autenticidad de la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$ es validada entonces en el segundo contexto de seguridad 7. El segundo procesador 19 en el segundo contexto de seguridad 7 es configurado para validar la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$. En un modo de realización en el que el certificado de generación C_{TSID} comprende un *hash* de la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$, la autenticidad de la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$, se valida mediante el cálculo del *hash* de la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$, y validando si se corresponde con el contenido en su certificado de generación C_{TSID}.

[0309] En el paso S903, el segundo contexto de seguridad 7 también puede validar que cualquier información de estado contenida en el mensaje cumple los requisitos.

[0310] Si la firma es verificada y la información de estado es validada, la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$, es almacenada en la segunda memoria de dispositivo 11 del segundo contexto de seguridad 7. Alternativamente, puede protegerse su integridad por el segundo contexto de seguridad 7 y almacenarse en un almacenamiento no de confianza fuera del segundo contexto de seguridad 7.

[0311] Si la firma no es verificada o la información de estado o clave no es validada, se devuelve un error a la fuente de tiempo 2, por ejemplo, se envía un mensaje indicando "Acceso denegado". En este momento, se termina la comunicación entre la fuente de tiempo 2 y el segundo contexto de seguridad 7.

[0312] En los pasos descritos anteriormente, el segundo contexto de seguridad 7 establece confianza con la fuente de tiempo de referencia 2. El segundo contexto de seguridad 7 establece confianza así con la fuente de tiempo 2 validando su origen, estado y autenticidad a través de una cadena de certificados.

[0313] Una vez que se haya establecido confianza, el segundo contexto de seguridad 7 solicita información de configuración de la fuente de tiempo 2 en el paso S904. El transceptor 15 en el segundo contexto de seguridad 7 envía un mensaje solicitando la información a la fuente de tiempo 2.

[0314] En el paso S905, en respuesta a la solicitud, la fuente de tiempo 2 genera información de configuración que incluye información relativa a la configuración de la fuente de tiempo 2, que puede incluir información de precisión sobre el reloj y ajustes de seguridad, las primitivas criptográficas que se han establecido, la versión del *software* que la fuente de tiempo utiliza y el estado de la fuente de tiempo 2, incluyendo cualquier anomalía detectada. El tercer procesador 41 en la fuente de tiempo 2 es configurado para generar este mensaje.

[0315] En el paso S906, el mensaje de respuesta es firmado por la mitad privada de la clave de identidad de la fuente de tiempo, $K_{TSID\ priv}$. El tercer procesador 41 en la fuente de tiempo 2 es configurado para firmar criptográficamente el mensaje con la mitad privada de la clave de identidad de la fuente de tiempo, $K_{TSID\ priv}$.

[0316] En el paso S907, la información de configuración y firma es enviada al segundo contexto de seguridad 7. El transceptor 39 en la fuente de tiempo 2 es configurado para enviar el mensaje firmado al segundo contexto de seguridad 7.

[0317] En el paso S908, el segundo contexto de seguridad 7 verifica la firma de respuesta utilizando la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$. El segundo procesador 19 en el segundo contexto de seguridad 5 es configurado para verificar la firma. La firma es verificada utilizando la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$. El segundo procesador 19 es configurado para llevar a cabo un algoritmo de verificación de firma que, dado el mensaje firmado y la clave pública $K_{TSID\ pub}$ acepte o rechace la declaración de autenticidad del mensaje.

[0318] En el paso S909, se realiza una comprobación sobre si la configuración de fuente de tiempo se encuentra dentro de tolerancias aceptables. La información de configuración es comprobada para validar que cumple los requisitos del proveedor de servicios.

[0319] La información de configuración puede comprobarse de nuevo siempre que se solicite un sello de tiempo por parte del segundo contexto de seguridad 7, mediante la solicitud de información de configuración de nuevo.

[0320] El estado y configuración de todos los dispositivos del sistema, es decir, el primer contexto de seguridad 5, el segundo contexto de seguridad 7 y la fuente de tiempo de referencia 2 pueden obtenerse a partir de la entrada de estado presente en el dispositivo. Tras la inicialización, cada dispositivo actualiza este campo y genera un nuevo mensaje de configuración para permitir a los clientes verificar de manera criptográfica los nuevos ajustes del dispositivo.

[0321] Si la firma es verificada con éxito y la configuración de la fuente de tiempo 2 se encuentra dentro de las tolerancias, el método avanza al paso S910. Si no, se devuelve un error a la fuente de tiempo 2, por ejemplo, se envía un mensaje indicando "Acceso denegado". En este momento, se termina la comunicación entre la fuente de tiempo 2 y el segundo contexto de seguridad 7.

[0322] En el paso S910, se envía un mensaje al primer contexto de seguridad 5 que comprende información que identifica la fuente de tiempo 2 e información que indica que la fuente de tiempo 2 es de confianza para el segundo contexto de seguridad 7. La información que identifica a la fuente de tiempo 2 puede comprender un número de identificación único, por ejemplo, el *hash* de la mitad pública de la clave de identidad de la fuente de tiempo 2 o la dirección IP de la fuente de tiempo 2. El transceptor 15 en el segundo contexto de seguridad 7 es configurado para enviar un mensaje que comprende información que identifica la fuente de tiempo 2 e información que indica que la fuente de tiempo es de confianza para el primer contexto de seguridad 5. La información que identifica la fuente de tiempo 2 y la información que indica que la fuente de tiempo 2 es de confianza también es almacenada en la memoria de dispositivo 11 del segundo contexto de seguridad 7, o fuera del segundo contexto de seguridad 7 de manera que se proteja su integridad.

[0323] En un modo de realización, el segundo contexto de seguridad 7 añade la fuente de tiempo 2 a una lista de fuente(s) de tiempo de confianza. La identificación única de la fuente de tiempo de referencia puede añadirse a la lista. La lista de fuente(s) de tiempo de confianza es transmitida entonces por el segundo contexto de seguridad 7. El primer contexto de seguridad 5 recibe la lista de fuente(s) de tiempo de confianza desde el segundo contexto de seguridad 7.

[0324] Dada la información recibida que identifica una o más fuentes de tiempo de confianza, el primer contexto de seguridad 5 puede consultar, y del mismo modo que el segundo contexto de seguridad 7, validar la autenticidad, estado y configuración de la(s) fuente(s) de tiempo. Se muestra un diagrama de flujo que ilustra este proceso en la figura 10. De nuevo, esto puede llevarse a cabo en cualquier momento como parte del método de transferencia de claves según un modo de realización de la presente invención, o como parte del método de control del uso de una clave criptográfica según un modo de realización de la presente invención.

[0325] Alternativamente, si la fuente de tiempo de referencia 2 es parte del primer contexto de seguridad 5, los pasos a continuación no se llevarán a cabo.

[0326] Además, en caso de que la fuente de tiempo de referencia 2 sea identificada en primer lugar por el primer contexto de seguridad 5, los pasos a continuación pueden llevarse a cabo, y después enviarse información sobre la fuente de tiempo 2 al segundo contexto de seguridad 7, que valida entonces la fuente de tiempo 2.

[0327] La transferencia de certificados criptográficos y claves criptográficas entre la fuente de tiempo de referencia 2 y el primer contexto de seguridad 5 descrita a continuación puede tener lugar a través de un canal seguro autenticado entre la fuente de tiempo de referencia 2 y el primer contexto de seguridad 5. Cuando la fuente de tiempo es proporcionada por el proveedor de servicios, el canal puede ser proporcionado y controlado por el proveedor de servicios o un *proxy*. Cuando la fuente de tiempo es proporcionada por un tercero proveedor de servicios de hora, el canal puede ser proporcionado directamente entre el inquilino y el proveedor de servicios de hora. Este canal puede ser proporcionado por el proveedor de servicios de hora o un *proxy*. Cabe observar que aunque el canal pueda estar protegido frente a terceros, está abierto a ataques por parte del proveedor de servicios de hora. La transferencia de certificados criptográficos y claves criptográficas entre la fuente de tiempo

de referencia 2 y el segundo contexto de seguridad 7 descrita a continuación puede tener lugar a través de un canal seguro autenticado entre la fuente de tiempo de referencia 2 y el segundo contexto de seguridad 7.

[0328] El intercambio de claves públicas y certificados descrito en relación con la figura 10 a continuación permite que se establezca una relación de confianza entre el primer contexto de seguridad 5 y la fuente de tiempo 2.

[0329] En el paso S1001, la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$, el certificado de generación $\{C_{TSID}\}_{Kman\ priv}$, y un certificado de configuración $\{C_{TSID}\}_{Kman\ priv}$ son enviados desde la fuente de tiempo de referencia 2 al primer contexto de seguridad 5 en respuesta a un mensaje de consulta del primer contexto de seguridad 5. Un transceptor 39 en la fuente de tiempo de referencia 2 es configurado para enviar la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$, y el certificado de generación $\{C_{TSID}\}_{Kman\ priv}$, al primer transceptor 13 en el primer contexto de seguridad 5. La información relativa al estado del dispositivo o dispositivos de fuente de tiempo puede enviarse en el mismo mensaje. La información relativa al estado del dispositivo o dispositivos también está contenida en el certificado de generación en este caso, para validar la información de estado.

[0330] En el paso S1002, el certificado de generación $\{C_{TSID}\}_{Kman\ priv}$ es verificado en el primer contexto de seguridad 5. El primer procesador 17 en el primer contexto de seguridad 5 es configurado para verificar el certificado de generación $\{C_{TSID}\}_{Kman\ priv}$. El certificado de generación es verificado utilizando la mitad pública de la clave de fabricante de confianza $K_{man\ pub}$. El primer procesador 17 es configurado para llevar a cabo un algoritmo de verificación de firma que, dado el mensaje firmado $\{C_{TSID}\}_{Kman\ priv}$ y la clave pública $K_{man\ pub}$ acepte o rechace la declaración de autenticidad del mensaje.

[0331] La autenticidad de la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$ es validada entonces en el primer contexto de seguridad 5. El primer procesador 17 en el primer contexto de seguridad 5 es configurado para validar la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$. En un modo de realización en el que el certificado de generación C_{TSID} comprende un *hash* de la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$, la autenticidad de la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$, es validada mediante el cálculo del *hash* de la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$, y validando que se corresponde con el contenido en su certificado de generación C_{TSID}.

[0332] En el paso S1003, el primer contexto de seguridad 5 puede validar también que el estado del dispositivo o dispositivos cumple los requisitos, a partir de cualquier información de estado contenida en el mensaje.

[0333] Si la firma es verificada y información de estado y clave es validada, la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$, es almacenada en la primera memoria de dispositivo 9 del primer contexto de seguridad 5. Alternativamente, puede protegerse su integridad por el primer contexto de seguridad 5 y almacenarse en un almacenamiento no de confianza fuera del primer contexto de seguridad 5.

[0334] Si la firma no es verificada o la información de estado o clave no es validada, se devuelve un error a la fuente de tiempo 2, por ejemplo, se envía un mensaje indicando "Acceso denegado". En este momento, se termina la comunicación entre la fuente de tiempo 2 y el primer contexto de seguridad 5.

[0335] En los pasos descritos anteriormente, el primer contexto de seguridad 5 establece confianza con la fuente de tiempo de referencia 2. El primer contexto de seguridad 5 establece confianza así con la fuente de tiempo 2 realizando una conexión segura a la fuente de tiempo, y validando su origen y autenticidad a través de una cadena de certificados.

[0336] Una vez se ha establecido la confianza, el primer contexto de seguridad 5 solicita información de estado y configuración de la fuente de tiempo 2 en el paso S1004. El transceptor en el primer contexto de seguridad 5 envía un mensaje solicitando la información a la fuente de tiempo 2.

[0337] En el paso S1005, en respuesta a la solicitud, la fuente de tiempo 2 genera un mensaje que incluye la configuración de la fuente de tiempo 2, que puede incluir información de precisión sobre el reloj y ajustes de seguridad, las primitivas criptográficas que se han establecido, la versión de *software* que la fuente de tiempo

utiliza y el estado de la fuente de tiempo, incluyendo cualquier anomalía detectada. El tercer procesador 41 en la fuente de tiempo es configurado para generar la información de configuración.

[0338] El mensaje puede ser el mismo mensaje enviado al segundo contexto de seguridad 7. Alternativamente, puede generarse un mensaje que contiene diferente información y enviarse de manera similar a la descrita en relación con la figura 2(b). El mensaje puede comprender información relativa a la configuración específica aplicada a la fuente de tiempo de referencia.

[0339] En el paso S1006, el mensaje de respuesta es firmado por la mitad privada de la clave de identidad de la fuente de tiempo, $K_{TSID\ priv}$. El tercer procesador 41 en la fuente de tiempo es configurado para firmar criptográficamente el mensaje con la mitad privada de la clave de identidad de la fuente de tiempo, $K_{TSID\ priv}$.

[0340] En el paso S1007, el mensaje y firma son enviados al primer contexto de seguridad 5. El transceptor 39 en la fuente de tiempo 2 es configurado para enviar el mensaje firmado al primer contexto de seguridad 5.

[0341] En el paso S1008, el primer contexto de seguridad 5 verifica la firma de respuesta utilizando la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$. El primer procesador 17 en el primer contexto de seguridad 5 es configurado para verificar la firma. La firma es verificada utilizando la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$. El primer procesador 17 es configurado para llevar a cabo un algoritmo de verificación de firma que, dado el mensaje firmado y la clave pública $K_{TSID\ pub}$ acepte o rechace la declaración de autenticidad del mensaje.

[0342] En el paso S1009, se realiza una comprobación sobre si la configuración de fuente de tiempo y el estado de fuente de tiempo se encuentran dentro de tolerancias aceptables. La información es comprobada para validar que cumple los requisitos del inquilino. En un modo de realización, la información de configuración es solicitada y comprobada inmediatamente antes de la transferencia de K_{tenant} al segundo contexto de seguridad 7. Esto asegura que se valida información de configuración actualizada.

[0343] Si la firma es verificada con éxito y la configuración y estado de la fuente de tiempo 2 se encuentran dentro de las tolerancias, la información que identifica la fuente de tiempo 2 y la información que indica que la fuente de tiempo 2 es de confianza se almacenan en la memoria de dispositivo 9 del primer contexto de seguridad 5, o fuera del primer contexto de seguridad 5 de manera que se proteja su integridad. Si no, se devuelve un error a la fuente de tiempo 2, por ejemplo, se envía un mensaje indicando "Acceso denegado". En este momento, se termina la comunicación entre la fuente de tiempo 2 y el primer contexto de seguridad 5.

[0344] La información de configuración puede comprobarse de nuevo siempre que se solicite un sello de tiempo por el primer contexto de seguridad 7, mediante la solicitud de información de configuración de nuevo.

[0345] La figura 11 es un diagrama de flujo que muestra un método de control de uso de una clave criptográfica, K_{tenant} según un modo de realización de la presente invención. La clave criptográfica, K_{tenant} se almacena de manera segura en el sistema de proveedor de servicios junto con una lista de control de acceso que especifica que una credencial de uso válida, por ejemplo, un certificado de uso, debe presentarse para permitir un primer tipo de uso de la clave criptográfica, K_{tenant}.

[0346] En un modo de realización alternativo, en lugar de la clave criptográfica, K_{tenant}, se almacena algún otro tipo de datos de manera segura en el sistema de proveedor de servicios, y se controla el uso de estos datos. Se almacena una lista de control de acceso junto con los datos, que especifica que debe presentarse un certificado de uso válido para permitir un primer tipo de uso de los datos. A continuación, los métodos y aparatos se describen en relación con el uso de una clave de inquilino, sin embargo, se entiende que algún otro tipo de datos puede ser sustituido por la clave de inquilino, y utilizarse del mismo modo.

[0347] El proceso de permitir el uso de una clave importada puede denominarse Autorización de Clave.

[0348] En el momento en el que el inquilino desea hacer que su clave esté disponible para el uso en la infraestructura criptográfica del proveedor de servicios, el inquilino genera un certificado de uso.

[0349] El paso S1101 comprende generar una credencial de uso en el primer contexto de seguridad 5. En un modo de realización, la credencial de uso es un certificado de uso. El procesador 17 en el primer contexto de seguridad 5 es configurado para generar el certificado de uso. El certificado de uso comprende información a partir de la cual puede identificarse la clave criptográfica K_{tenant} correspondiente al certificado de uso e información a partir de la cual puede determinarse la expiración del certificado de uso.

[0350] En un modo de realización, la información a partir de la cual puede identificarse la clave criptográfica K_{tenant} correspondiente al certificado de uso comprende el *hash* de K_{tenant}.

[0351] En un modo de realización, la información a partir de la cual puede determinarse la expiración del certificado de uso comprende un tiempo de expiración, e información que identifique una fuente de tiempo de referencia. El tiempo de expiración se calcula en relación con una fuente de tiempo de referencia 2 que es de confianza para ambos el primer contexto de seguridad 5 y el segundo contexto de seguridad 7. La confianza en una fuente de tiempo de referencia es comprobada por el primer contexto de seguridad 5 y el segundo contexto de seguridad 7 conectándose de manera independiente a la fuente de tiempo de referencia y validando que la fuente de tiempo es de confianza y que la fuente de tiempo es a prueba de manipulaciones a través del parámetro de estado de módulo del certificado. Esto se ha descrito anteriormente en relación con las figuras 9 y 10 y puede llevarse a cabo antes del método de transferencia de clave, o después del método de transferencia de clave y antes de la generación de un certificado de uso, por ejemplo.

[0352] Por tanto, el certificado de uso comprende información acerca de un periodo de validez en relación con una fuente de tiempo segura 2.

[0353] De este modo, la Autorización de Clave comienza con un inquilino que genera un certificado de credencial, o un certificado "uso-clave" que se corresponde con el definido en un permiso de K_{tenant}, la ACL. En otras palabras, el certificado de uso cumple los requisitos que son definidos en la lista de control de acceso correspondiente a K_{tenant}.

[0354] En un modo de realización, el certificado de credencial, o certificado de uso, es firmado con la mitad privada de $K_{tenant\text{-}sign}$.

[0355] La figura 12 muestra un método para generar un certificado de uso en el primer contexto de seguridad 5, que es parte de un método de control de uso de una clave criptográfica, K_{tenant} según un modo de realización de la presente invención.

[0356] En el paso S1201, una fuente de tiempo de referencia 2 es seleccionada por el primer contexto de seguridad 5. La información que identifica una o más fuentes de tiempo e información que indica que la fuente o fuentes de tiempo son de confianza puede almacenarse en la memoria de dispositivo 9 del primer contexto de seguridad 5 o fuera del primer contexto de seguridad de manera que se proteja su integridad. Una de las fuentes de tiempo es seleccionada por el primer contexto de seguridad 5.

[0357] La fuente de tiempo 2 puede elegirse de una lista de fuentes de tiempo de confianza transmitida por el segundo contexto de seguridad 7 y para la cual el primer contexto de seguridad 5 ha establecido confianza. De este modo, tanto el segundo contexto de seguridad 7 como el primer contexto de seguridad 5 han establecido confianza con una o más fuentes de tiempo en la lista. Cada una de estas fuentes de tiempo son fuentes de tiempo válidas con el estado y configuración necesarios. El primer contexto de seguridad selecciona una fuente de tiempo 2 de la lista de una o más fuentes de tiempo válidas.

[0358] En el paso S1202, el primer contexto de seguridad 5 solicita el sello de tiempo actual de la fuente de tiempo escogida 2. El primer transceptor 13 en el primer contexto de seguridad 5 envía un mensaje de solicitud a la fuente de tiempo 2.

[0359] En el paso S1203 la fuente de tiempo 2 genera un mensaje que incluye el sello de tiempo. El mensaje puede comprender información que identifica la fuente de tiempo y la hora actual en la generación del mensaje, determinada a partir del reloj de la fuente de tiempo. La información que identifica la fuente de tiempo puede comprender el *hash* de la clave de identidad pública de la fuente generadora de tiempo, $K_{TSID\ pub}$.

[0360] El mensaje puede comprender además la información de configuración actual, relativa a cualquier indicación de que la fuente de tiempo haya sido manipulada, por ejemplo. Esta información puede ser utilizada entonces por el cliente para comprobar si la fuente de tiempo se encuentra en un estado aceptable antes de utilizar el sello de tiempo en el certificado de uso.

[0361] En el paso S1204, el mensaje es firmado con la mitad privada de la clave de identidad de la fuente de tiempo, $K_{TSID\ priv}$. El tercer procesador 41 en la fuente de tiempo es configurado para firmar criptográficamente el mensaje con la mitad privada de la clave de identidad de la fuente de tiempo, $K_{TSID\ priv}$.

[0362] En el paso S1205, el mensaje y firma son enviados al primer contexto de seguridad 5. El transceptor 39 en la fuente de tiempo 2 es configurado para enviar el mensaje firmado al primer contexto de seguridad 5.

[0363] En el paso S1206, el primer contexto de seguridad 5 verifica la firma de respuesta utilizando la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$. El primer procesador 17 en el primer contexto de seguridad 5 es configurado para verificar la firma. La firma es verificada utilizando la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$. El primer procesador 17 es configurado para llevar a cabo un algoritmo de verificación de firma que, dado el mensaje firmado y la clave pública $K_{TSID\ pub}$ acepte o rechace la declaración de autenticidad del mensaje. Si la firma es verificada con éxito, el método avanza al paso S1207. Si no, se devuelve un error a la fuente de tiempo 2, por ejemplo, se envía un mensaje indicando "Acceso denegado". En este momento, se termina la comunicación entre la fuente de tiempo 2 y el segundo contexto de seguridad 7.

[0364] Si la información de configuración es incluida en el mensaje, el primer contexto de seguridad 5 valida que la configuración sea aceptable. Si la información de configuración actual no es aceptable para el inquilino, entonces se para la generación del certificado de uso.

[0365] En el paso S1207 el inquilino calcula el tiempo de expiración para su clave K_{tenant} basándose en el sello de tiempo antes mencionado. El tiempo de expiración se calcula como la hora del sello de tiempo más una cantidad de tiempo durante la que el inquilino desea que el certificado esté activo, por ejemplo, la hora del sello de tiempo más uno o más días.

[0366] Cuando el tiempo de expiración es corto en comparación con el retraso de comunicación, un retraso de comunicación puede tenerse en cuenta en el tiempo de expiración, por ejemplo. En este caso, el tiempo de expiración es calculado como la hora del sello de tiempo más el retraso de comunicación de la fuente de tiempo de referencia 2 al primer contexto de seguridad 5 más el retraso de comunicación del primer contexto de seguridad 5 al segundo contexto de seguridad 7 más la cantidad de tiempo durante el que el inquilino desea que el certificado esté activo.

[0367] La cantidad de tiempo durante el que el inquilino desea que el certificado esté activo puede ser pocos segundos o varios días, por ejemplo, según la aplicación.

[0368] Puede incluirse también un "tiempo de inicio" en el certificado de uso, de manera que el certificado de uso define un periodo de validez, dentro del cual el certificado es válido. Esto permite a un inquilino pregenerar uno o más certificados con antelación a su uso.

[0369] En el paso S1208, se incluyen el tiempo de expiración, una referencia a la fuente de tiempo, una referencia a K_{tenant} y una referencia al segundo contexto de seguridad 7 en un certificado de uso.

[0370] Una referencia a un componente de sistema, como la fuente de tiempo o el segundo contexto de seguridad 7 puede ser un ID único que puede estar vinculado al mismo utilizando un certificado, o puede ser el *hash* de la mitad pública de su clave de identidad K_{ID}.

[0371] El procesador 17 en el primer contexto de seguridad 5 es configurado para generar un certificado de uso, que comprende el tiempo de expiración calculado en el paso S1207, una referencia a una fuente de tiempo, una referencia a K_{tenant} y una referencia al segundo contexto de seguridad 7.

[0372] En un modo de realización, la referencia a K_{tenant} es el *hash* de K_{tenant}. En un modo de realización, la referencia a la fuente de tiempo 2 es el *hash* de la mitad pública de su clave de identidad $K_{TSID-pub}$. En un modo de realización, la referencia al segundo contexto de seguridad 7 es el *hash* de la mitad pública de su clave de identidad $K_{2ID-pub}$.

[0373] Volviendo a la figura 11, una vez que se ha generado el certificado de uso, se emite junto con información a partir de la cual puede identificarse el origen del certificado de uso. En un modo de realización, la información a partir de la cual puede identificarse el origen del certificado de uso es un *hash* de $K_{tenant-signpub}$.

[0374] En el paso S1102, el certificado de uso es firmado con la mitad privada de la clave de firma $K_{tenant-sign\ priv}$. El primer procesador 17 en el primer contexto de seguridad 5 es configurado para firmar criptográficamente el certificado con la mitad privada de la clave de firma $K_{tenant-sign\ priv}$.

[0375] En el paso S1103, el certificado de uso es enviado al servidor de aplicaciones del proveedor de servicios, junto con información a partir de la cual puede validarse el origen del certificado de uso. La información a partir de la cual puede validarse el origen del certificado de uso es la firma, es decir, el certificado de uso firmado.

[0376] El primer transceptor 13 es configurado para enviar el certificado de uso al servidor de aplicaciones. Puede enviarse un certificado de uso a otras entidades que deseen utilizar la clave de inquilino. Estas entidades pueden comunicarse directamente con el segundo contexto de seguridad 7 o a través del servidor de aplicaciones.

[0377] La información a partir de la cual puede identificarse el origen del certificado de uso también puede enviarse con el certificado de uso. La información a partir de la cual puede identificarse el origen del certificado de uso puede ser un *hash* de $K_{tenant-signpub}$. Se incluye información a partir de la cual puede identificarse el origen del certificado de uso para identificar qué clave de firma debería utilizarse para verificar la firma.

[0378] El primer contexto de seguridad 5 envía así el certificado de uso, la firma y el *hash* de $K_{tenant-sign\ pub}$, al proveedor de servicios. Cada uso de la clave por el proveedor de servicios es acompañado entonces por la presentación de esta información al segundo contexto de seguridad 7.

[0379] En el paso S1104, el certificado de uso, firma y la información a partir de la cual puede identificarse el origen del certificado de uso, que puede ser el *hash* de $K_{tenant-signpub}$ es presentada al segundo contexto de seguridad 7 por el servidor de aplicaciones. El certificado de uso se presenta cada vez que el servidor de aplicaciones quiere usar K_{tenant}. El servidor de aplicaciones puede enviar un mensaje de solicitud, especificando el uso de la clave de inquilino que es requerido, junto con el certificado de uso. Por ejemplo, el servidor de aplicaciones puede enviar un mensaje al segundo contexto de seguridad 7 que comprende un archivo de datos, una solicitud para que segundo contexto de seguridad 7 cifre el archivo de datos con la clave de inquilino, un certificado de uso, y la información a partir de la cual pueda identificarse el origen del certificado de uso, que puede ser el *hash* de $K_{tenant-signpub}$.

[0380] El segundo contexto de seguridad 7 puede tener acceso a un número de claves públicas, por ejemplo, asociadas a distintos inquilinos. Las claves pueden almacenarse en el segundo contexto de seguridad 7, o fuera del segundo contexto de seguridad 7 de manera autenticada. El segundo contexto de seguridad 7 identifica la clave de verificación de firma correcta $K_{tenant-signpub}$, basándose en la información a partir de la cual puede identificarse el origen del certificado de uso, que puede ser el *hash* de $K_{tenant-signpub}$. A continuación, el certificado de uso firmado es verificado en el segundo contexto de seguridad 7. El segundo procesador 19 en el segundo contexto de seguridad 7 es configurado para verificar la firma. La firma se verifica utilizando la mitad pública de la clave de firma $K_{tenant-sign\ pub}$. El segundo procesador 19 es configurado para llevar a cabo un algoritmo de verificación de firma que, dado el certificado de uso firmado y la clave pública $K_{tenant-sign\ pub}$ acepte o rechace la declaración de autenticidad del mensaje. Si la firma es verificada con éxito, el método avanza al paso S1105. Si no, se devuelve un error al primer contexto de seguridad 5, por ejemplo, se envía un mensaje indicando "Acceso denegado". En este momento, se termina la comunicación entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7.

[0381] En el paso S1105, el segundo contexto de seguridad 7 valida el certificado de uso con respecto a la lista de control de acceso almacenada en la segunda memoria de dispositivo 11. Como parte de este paso, se valida que el certificado de uso no ha expirado. También se valida que el certificado de uso permita la operación que se

solicita, en otras palabras, que el certificado de uso se corresponda con la credencial asociada al permiso correspondiente a la operación o uso que se solicita. El segundo procesador 19 es configurado para validar el certificado de uso. Si el certificado no es válido, por ejemplo, debido a manipulación indicada por la firma de certificado, expiración o si la ACL no permite la operación solicitada, entonces el segundo contexto de seguridad 7 puede devolver un mensaje de error al servidor de aplicaciones, por ejemplo.

[0382] El segundo contexto de seguridad 7 identifica la clave de inquilino almacenada de manera segura correspondiente al certificado de uso a partir de la referencia a K_{tenant} en el certificado de uso.

[0383] El segundo contexto de seguridad carga la clave de inquilino almacenada de forma segura y la ACL. La carga de la clave de inquilino implica que esté disponible para el procesador en el segundo contexto de seguridad 7, es decir, enviar la clave de inquilino y ACL a la memoria de dispositivo 9, si no está ya presente. Esto puede implicar cargar la clave de inquilino y ACL desde un dispositivo de memoria no volátil fuera del segundo contexto de seguridad 7, descifrar la clave y hacer que esté disponible para el segundo procesador, por ejemplo.

[0384] En este momento, el segundo contexto de seguridad 7 valida el certificado de uso y que el tiempo de expiración no haya transcurrido con respecto a la fuente de tiempo de referencia. El segundo contexto de seguridad 7 puede utilizar el certificado de uso para habilitar el permiso correspondiente validando que todos los campos dados son los esperados.

[0385] El segundo procesador 19 es configurado para confirmar que la referencia a K_{tenant} y la referencia al segundo contexto de seguridad 7 se corresponden con aquellas en la ACL correspondiente a la clave K_{tenant} y almacenadas en la segunda memoria de dispositivo 11. En un modo de realización, la referencia a K_{tenant} es el *hash* de K_{tenant}. En un modo de realización, la referencia al segundo contexto de seguridad 7 es el *hash* de la mitad pública de la clave de identidad $K_{2ID\ pub}$.

[0386] Si la referencia a K_{tenant} y la referencia al segundo contexto de seguridad 7 se corresponde con aquellas en la ACL, se confirma si el periodo de validez ha expirado. Si no, se devuelve un error al servidor de aplicaciones, por ejemplo, se envía un mensaje indicando "Certificado expirado".

[0387] El segundo procesador 19 se configura además para confirmar que el periodo de validez no ha expirado con respecto a la fuente de tiempo referenciada 2. En un modo de realización, el segundo contexto de seguridad 7 solicita el sello de tiempo actual de la fuente de tiempo 2 correspondiente a la referencia en el certificado de uso. El segundo transceptor 15 en el segundo contexto de seguridad 7 es configurado para enviar un mensaje de solicitud a la fuente de tiempo 2. En respuesta al mensaje de solicitud, la fuente de tiempo 2 genera un mensaje que incluye el sello de tiempo actual. El mensaje es firmado con la mitad privada de la clave de identidad de la fuente de tiempo, $K_{TSID\ priv}$. El tercer procesador 41 en la fuente de tiempo es configurado para firmar criptográficamente el mensaje con la mitad privada de la clave de identidad de la fuente de tiempo, $K_{TSID\ priv}$. A continuación, el mensaje firmado es enviado al segundo contexto de seguridad 7. El transceptor 39 en la fuente de tiempo 2 es configurado para enviar el mensaje firmado al segundo contexto de seguridad 7. El mensaje puede comprender también la información de configuración actual de la fuente de tiempo.

[0388] El segundo contexto de seguridad 7 verifica entonces la firma de respuesta utilizando la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$. El segundo procesador 19 en el segundo contexto de seguridad 7 es configurado para verificar la firma. La firma es verificada utilizando la mitad pública de la clave de identidad de la fuente de tiempo, $K_{TSID\ pub}$. El segundo procesador 19 es configurado para llevar a cabo un algoritmo de verificación de firma que, dado el mensaje firmado y la clave pública $K_{TSID\ pub}$ acepte o rechace la declaración de autenticidad del mensaje.

[0389] Si la firma es verificada con éxito, el sello de tiempo actual es comparado con el tiempo de expiración contenido en el certificado de uso para determinar si el certificado de uso ha expirado. Si no, se devuelve un error al servidor de aplicaciones, por ejemplo, se envía un mensaje indicando "Acceso denegado". En este momento, se termina la comunicación entre el primer contexto de seguridad 5 y el segundo contexto de seguridad 7.

[0390] Si el sello de tiempo actual recibido de la fuente de tiempo 2 es anterior al tiempo de expiración contenido en el certificado de uso, entonces el método avanza al paso S1106. Si no, se devuelve un error al servidor de

aplicaciones, por ejemplo, se envía un mensaje indicando "Certificado expirado". A continuación, el servidor de aplicaciones puede solicitar al primer contexto de seguridad 5 que proporcione un nuevo certificado o simplemente terminar la operación.

[0391] En el paso S1106, el segundo contexto de seguridad 7 permite el uso de la clave criptográfica, K_{tenant}, con la condición de que el certificado de uso sea válido y no haya expirado. Si el certificado es válido y el tiempo de expiración no ha transcurrido todavía, se permite que proceda la operación criptográfica. El segundo contexto de seguridad 7 puede utilizar ahora la clave de inquilino dentro del periodo de validez. El segundo contexto de seguridad 7 activa los permisos necesarios dentro de la ACL correspondientes al uso solicitado y comprueba la ACL para buscar un permiso activo que permita la solicitud. A continuación, el segundo contexto de seguridad 7 lleva a cabo la operación solicitada y devuelve el resultado al servidor de aplicaciones. Por ejemplo, en caso de que el servidor de aplicaciones haya enviado un mensaje que comprende un archivo de datos y una solicitud de que el segundo contexto de seguridad 7 cifre el archivo de datos con la clave de inquilino, el segundo contexto de seguridad 7 cifra el archivo de datos con la clave de inquilino y devuelve el archivo de datos cifrado al servidor de aplicaciones.

[0392] En el momento de expiración o antes, el inquilino puede generar un nuevo certificado para extender el tiempo de expiración de la clave. La falta de regeneración de un nuevo certificado provoca que la clave sea inutilizable por parte del proveedor de servicios. En un modo de realización, el segundo contexto de seguridad 7 notifica al primer contexto de seguridad 5 antes o en el momento de expiración del certificado de uso. Puede generarse entonces un nuevo certificado de uso en el primer contexto de seguridad con un tiempo de expiración posterior. Alternativamente, el segundo contexto de seguridad 7 notifica al servidor de aplicaciones antes o en el momento de expiración del certificado de uso. A continuación, el servidor de aplicaciones solicita un nuevo certificado de uso del primer contexto de seguridad 5. Alternativamente, el certificado de uso es leído por el servidor de aplicaciones, que solicita un nuevo certificado de uso del primer contexto de seguridad 5 antes o en el momento de expiración. Alternativamente, un componente adicional, que puede ser propiedad del inquilino o del proveedor de servicios puede monitorizar certificados y elevar una solicitud de certificados cuando están cerca de expirar o han expirado.

[0393] De este modo, el sistema de inquilino 1 concede de manera efectiva la clave criptográfica K_{tenant} al sistema de proveedor de servicios 3 de manera segura. El uso de la clave por el proveedor de servicios es limitado criptográficamente por un tiempo de expiración con respecto a una fuente de tiempo de confianza, según establece el inquilino propietario en el certificado de uso. La ACL especifica que el uso de la clave criptográfica K_{tenant} solo se permite cuando se facilita un certificado de uso no expirado. Además, el inquilino puede restringir cómo es utilizada la clave por el proveedor de servicios.

[0394] La figura 13 es una ilustración esquemática de un método de control de uso de una clave criptográfica, K_{tenant} según un modo de realización de la presente invención.

[0395] Este método mostrado corresponde al caso en el que la clave de inquilino está siendo utilizada en el segundo contexto de seguridad 7 y transcurre el periodo de expiración. El segundo contexto de seguridad 7 o el servidor de aplicaciones pueden comparar periódicamente la hora actual obtenida de la fuente de tiempo de referencia 2 con el tiempo de expiración en el certificado de uso y a partir de esta información determinar si el certificado ha expirado. Alternativamente, el segundo contexto de seguridad 7 puede determinar que el certificado ha expirado solo cuando se realice una solicitud que utilice un certificado expirado. El segundo contexto de seguridad 7 puede notificar al primer contexto de seguridad 5, el servidor de aplicaciones o un dispositivo adicional que la clave ha expirado.

[0396] El primer contexto de seguridad 5 es configurado para enviar un mensaje de solicitud a la fuente de tiempo 2 en respuesta a la notificación, solicitando el sello de tiempo actual según se ha descrito anteriormente en relación con el paso S1202.

[0397] La fuente de tiempo 2 es configurada para generar y enviar un mensaje que comprende la información de tiempo como se ha descrito anteriormente en relación con los pasos del 1203 a 1205.

[0398] El mensaje es verificado en el primer contexto de seguridad 5 según se ha descrito anteriormente en relación con el paso S1206 y se genera un certificado de uso según se ha descrito en los pasos del S1207 al S1208 y se firma según se ha descrito anteriormente en el paso S1102. El certificado de uso es enviado al

proveedor de servicios según se ha descrito anteriormente en el paso S1103, y enviado al segundo contexto de seguridad 7 y verificado en el segundo contexto de seguridad 7 según se ha descrito en relación con el paso S1104. Se carga la clave de inquilino almacenada correspondiente al certificado de uso y se obtiene el sello de tiempo actual de la fuente de tiempo 2 y se valida según se ha descrito anteriormente en relación con S1105. La carga de la clave de inquilino implica que esté disponible para el procesador, es decir, enviar a la memoria de dispositivo 9, si no está ya presente. Esto puede implicar cargar la clave de inquilino del dispositivo de memoria no volátil fuera del segundo contexto de seguridad 7, descifrar la clave y hacer que esté disponible para el procesador. A continuación, la clave es activada como en el paso S1106 anterior.

[0399] La figura 14 es una ilustración esquemática de un método de control de uso de una clave criptográfica, K_{tenant} según un modo de realización de la presente invención.

[0400] En el paso inicial, el primer contexto de seguridad 5 obtiene el certificado de generación de la fuente de tiempo, el estado y la hora de una fuente de tiempo 2. A continuación, se verifica la firma del sello de tiempo y el certificado de generación en el primer contexto de seguridad 5. Esto se ha descrito anteriormente en relación con la figura 10 y en los pasos del S1201 al S1206.

[0401] Si se valida la firma del sello de tiempo y certificado de generación, entonces el método avanza al siguiente paso, "generar un certificado de autorización". Si no, se devuelve un error.

[0402] El certificado de uso es generado como se ha descrito anteriormente en los pasos S1207 y S1208. A continuación, se envía el certificado de uso al segundo contexto de seguridad 7, como se ha descrito anteriormente en relación con el paso S1103.

[0403] Los pasos descritos anteriormente definen un sistema que está protegido de ataques de terceros, así como de un proveedor de servicios malicioso, puesto que todo el material de claves es cifrado entre el inquilino y el segundo contexto de seguridad 7, el material de clave de inquilino es almacenado en formato seguro y a prueba de manipulaciones, las claves de inquilino solo pueden utilizarse cuando es autorizado por un inquilino de una manera que se implemente criptográficamente, y se evita la suplantación de identidad de componentes o *spoofing* por la presencia de una clave de identidad K_{ID} y certificado de generación firmado por un fabricante de confianza tanto para el inquilino como para el proveedor de servicios.

[0404] El método de transferencia de claves y método de control de uso de la clave anteriormente descritos significan que el inquilino puede conceder claves criptográficas de manera segura a un proveedor de servicios que está alojando una infraestructura criptográfica compartida de origen conocido. El uso de la clave de inquilino permanece bajo el control del inquilino de manera criptográficamente protegida.

[0405] Como parte del método de transferencia de clave, el inquilino genera una clave dentro de un dispositivo seguro autoalojado, el primer contexto de seguridad 5.

[0406] El dispositivo seguro del inquilino, el primer contexto de seguridad 5, valida que la infraestructura criptográfica alojada por un proveedor de servicios escogido, el segundo contexto de seguridad 7, se adhiere a un conjunto de normas aceptables para el inquilino validando que la infraestructura está construida utilizando un fabricante de confianza, configurada de manera aceptable para el inquilino y adecuada para concederle una clave. El paso S205 descrito anteriormente en relación con la figura 2(a) permite la validación de que la infraestructura se ha construido utilizando un fabricante de confianza. Si la firma del certificado de generación C_{2ID} es verificada, entonces se valida que el segundo contexto de seguridad está construido por un fabricante de confianza. El paso S215 descrito anteriormente en relación con la figura 2(b) permite la validación de que la infraestructura está configurada de una manera que es aceptable para el inquilino y adecuada para concederle una clave.

[0407] Además, el inquilino y la infraestructura criptográfica del proveedor de servicios utilizan una fuente de tiempo de confianza 2, que puede estar alojada por un tercero, para aplicar los tiempos de expiración de clave establecidos por el inquilino.

[0408] Los dispositivos y métodos descritos anteriormente permiten que un proveedor de servicios en la nube (CSP, por sus siglas en inglés) proporcione una solución criptográfica alojada multitenencia. El sistema está diseñado para estar protegido de ataques por parte de terceros y el propio CSP. Un inquilino conserva el control

de su clave, proporcionando autorizaciones de uso, que son aplicadas criptográficamente, para su uso dentro de un sistema alojado por el CSP. Permite tanto la multitenencia de HSM como seguridad para las claves transferidas a una infraestructura criptográfica del proveedor de servicios. Más de un inquilino puede utilizar un solo dispositivo criptográfico. No obstante, se protege la seguridad de una clave de inquilino frente a terceros y el proveedor de servicios.

[0409] Los métodos y dispositivos anteriormente descritos permiten a un inquilino que conceda de manera verificable claves criptográficas para su uso dentro de una infraestructura criptográfica del proveedor de servicios de manera que es inaccesible para el proveedor de servicios y terceros, al tiempo que mantiene el control sobre el uso de las claves una vez dentro del contexto de seguridad del CSP. Esto permite la concesión segura de claves criptográficas entre un inquilino y un proveedor de servicios, con la capacidad de limitar el uso de una clave de inquilino para su uso dentro de un HSM del proveedor de servicios durante un periodo de tiempo establecido, y proporcionando resistencia a ataques de administradores deshonestos o maliciosos. Permite la concesión de claves a un CSP de un modo que se implementa criptográficamente. Permite a los proveedores de servicios alojar servicios multitenencia que son sólidos frente a ataques de terceros al tiempo que también son sólidos frente a CSP maliciosos. Implementar criptográficamente que el uso de una clave de inquilino sea controlado por el inquilino asegura que el uso de las claves está completamente controlado ahora por los inquilinos, volviendo el servicio seguro frente a ataques y permitiendo compartir la infraestructura con otros.

[0410] Los dispositivos y métodos descritos anteriormente permiten a un CSP proporcionar a sus inquilinos el uso de su infraestructura criptográfica para aplicaciones como pagos, seguridad y regulación.

[0411] El segundo contexto de seguridad 7 es parte de un sistema de proveedor de servicios, que permite al proveedor de servicios, por ejemplo, un CSP, alojar servicios criptográficos a través de módulos de seguridad de *hardware*, HSM, en nombre de sus clientes.

[0412] Aunque se han descrito determinados modos de realización, estos modos de realización se han presentado a modo de ejemplo únicamente y no pretenden limitar el alcance de la invención. De hecho, los métodos y aparados novedosos descritos aquí pueden implementarse en una variedad de formas diferentes; además, pueden realizarse diversas omisiones, sustituciones y cambios en la forma de los métodos y los aparatos descritos aquí sin salir del alcance de la invención tal y como es reivindicada. Las reivindicaciones que acompañan y sus equivalentes pretenden cubrir tales formas de modificaciones que recaen dentro del alcance de la invención tal y como es reivindicada.

REIVINDICACIONES

1. Un método de transferencia de datos entre un primer contexto de seguridad (5) en un sistema de inquilino (1) y un segundo contexto de seguridad (7) en un sistema de proveedor de servicios (3), comprendiendo el método:

generar una lista de control de acceso que corresponde a los datos en el primer contexto de seguridad (5), donde la lista de control de acceso especifica que debe presentarse una credencial de uso válida para permitir un primer tipo de uso de los datos;

generar un primer par de claves criptográficas y un primer certificado criptográfico en el segundo contexto de seguridad (7), comprendiendo el primer par de claves criptográficas una primera clave pública, $K_{BLOB\ pub}$, y una primera clave privada, $K_{BLOB\ priv}$ y el primer certificado criptográfico comprendiendo información a partir de la cual el origen de la primera clave pública $K_{BLOB\ pub}$ puede ser validado;

enviar la primera clave pública $K_{BLOB\ pub}$ y el primer certificado criptográfico al primer contexto de seguridad (5);

validar el primer certificado criptográfico en el primer contexto de seguridad (5);

si el primer certificado criptográfico es válido, cifrar los datos y la lista de control de acceso correspondiente con la primera clave pública $K_{BLOB\ pub}$ en el primer contexto de seguridad (5);

enviar los datos y lista de control de acceso correspondiente cifrados, e información a partir de la cual el origen de los datos puede validarse, al segundo contexto de seguridad (7).

2. El método según la reivindicación 1, donde los datos comprenden una clave criptográfica, K_{tenant}.

3. El método según la reivindicación 2, que comprende además la etapa de generar la clave criptográfica, K_{tenant} en el primer contexto de seguridad (5).

4. El método según la reivindicación 3, que comprende además:

validar, en el segundo contexto de seguridad (7), el origen de la clave criptográfica K_{tenant};

descifrar la clave criptográfica K_{tenant} y la lista de control de acceso correspondiente cifradas con la primera clave privada $K_{BLOB\ priv}$ en el segundo contexto de seguridad (7).

5. El método según la reivindicación 4, que comprende además:

recifrar la clave criptográfica K_{tenant} con una clave criptográfica adicional en el segundo contexto de seguridad (7), donde la clave criptográfica adicional no puede dejar el segundo contexto de seguridad (7);

almacenar la clave criptográfica recifrada K_{tenant}, lista de control de acceso correspondiente, e información a partir de la cual el origen de la clave criptográfica K_{tenant} puede validarse.

6. El método según cualquiera de las reivindicaciones de la 2 a la 5, donde el primer tipo de uso son una o más operaciones criptográficas.

7. El método según cualquiera de las reivindicaciones de la 2 a la 6, que comprende además:

validar en el primer contexto de seguridad (5) que el segundo contexto de seguridad (7) es fabricado por un fabricante de confianza, que la configuración del segundo contexto de seguridad (7) cumple los requisitos de seguridad del inquilino y que el segundo contexto de seguridad (7) está configurado para aplicar las políticas contenidas en la ACL.

8. El método según cualquiera de las reivindicaciones de la 2 a la 7, donde el segundo contexto de seguridad (7) almacena una segunda clave privada de identidad, $K_{2ID\ priv}$, comprendiendo además el método:

enviar una segunda clave pública de identidad, $K_{2ID\ pub}$, y un segundo certificado de identidad desde el segundo contexto de seguridad (7) al primer contexto de seguridad (5), donde la segunda clave pública de identidad, $K_{2ID\ pub}$ y la segunda clave privada de identidad, $K_{2ID\ priv}$ son un par de claves criptográficas y el segundo certificado de identidad comprende información que identifica $K_{2ID\ pub}$ y está firmado de manera criptográfica por una clave privada de fabricante $K_{man\ priv}$.

9. El método según la reivindicación 8, que comprende además:

generar información relativa a la configuración actual del segundo contexto de seguridad (7);

firmar criptográficamente la información con la segunda clave privada de identidad, $K_{2ID\ priv}$,

enviar la información firmada desde el segundo contexto de seguridad (7) al primer contexto de seguridad (5).

10. El método según la reivindicación 9, donde el primer certificado criptográfico comprende la información relativa a la configuración actual del segundo contexto de seguridad (7) y es firmado con la segunda clave privada de identidad, $K_{2ID\ priv}$.

11. El método según cualquiera de las reivindicaciones de la 8 a la 10, donde el primer contexto de seguridad (5) almacena una primera clave privada de identidad, $K_{1ID\ priv}$, comprendiendo además el método:

enviar una primera clave pública de identidad, $K_{1ID\ pub}$, y un primer certificado de identidad desde el primer contexto de seguridad (5) al segundo contexto de seguridad (7), donde la primera clave pública de identidad, $K_{1ID\ pub}$ y la primera clave privada de identidad, $K_{1ID\ priv}$ son un par de claves criptográficas y el primer certificado de identidad comprende información que identifica $K_{1ID\ pub}$ y está firmado de manera criptográfica por una clave privada de fabricante $K_{man\ priv}$.

12. El método según la reivindicación 11, que comprende además:

generar un segundo par de claves criptográficas y un segundo certificado criptográfico en el primer contexto de seguridad (5), comprendiendo el segundo par de claves criptográficas una segunda clave pública, $K_{tenant\text{-}signpub}$, y una segunda clave privada, $K_{tenant\text{-}signpriv}$ y el segundo certificado criptográfico comprendiendo información a partir de la cual el origen de la segunda clave pública $K_{tenant\text{-}signpub}$ puede ser identificado;

firmar criptográficamente el segundo certificado criptográfico con la primera clave privada de identidad, $K_{1ID\ priv}$;

enviar la segunda clave pública $K_{tenant\text{-}signpub}$ y el segundo certificado criptográfico firmado al segundo contexto de seguridad (7);

verificar el segundo certificado criptográfico utilizando la primera clave pública de identidad, $K_{1ID\ pub}$.

13. El método según la reivindicación 12, donde la lista de control de acceso especifica que la credencial de uso es un certificado de uso que es firmado por la segunda clave privada $K_{tenant\text{-}signpriv}$ para permitir el primer tipo de uso de la clave criptográfica, K_{tenant}.

14. El método de transferencia de claves criptográficas según las reivindicaciones 12 o 13, donde la información a partir de la cual el origen de la clave criptográfica K_{tenant} puede validarse comprende la clave criptográfica K_{tenant} y la lista de control de acceso correspondiente cifradas, firmadas con $K_{tenant\text{-}signpriv}$.

15. El método según la reivindicación 14, donde la etapa de enviar la clave criptográfica K_{tenant} y lista de control de acceso correspondiente cifradas, e información a partir de la cual el origen de la clave criptográfica K_{tenant} puede validarse, al segundo contexto de seguridad (7) comprende:

firmar criptográficamente la clave criptográfica K_{tenant} y la lista de control de acceso correspondiente cifradas con $K_{tenant\text{-}signpriv}$;

enviar la clave criptográfica K_{tenant} y lista de control de acceso correspondiente cifradas, la firma de la clave criptográfica K_{tenant} y lista de control de acceso correspondiente cifradas y el *hash* de $K_{tenant\text{-}signpub}$ al segundo contexto de seguridad (7).

16. El método según cualquiera de las reivindicaciones de la 2 a la 15, donde la lista de control de acceso especifica que la credencial de uso debe comprender información a partir de la cual pueda determinarse la expiración de la credencial de uso y no debe haber expirado para ser válida.

17. El método según cualquiera de las reivindicaciones de la 2 a la 16, donde la lista de control de acceso especifica que la clave criptográfica, K_{tenant} solo puede ser cifrada para su almacenamiento fuera del segundo contexto de seguridad (7) mediante una clave que no puede salir del segundo contexto de seguridad.

18. El método según cualquiera de las reivindicaciones de la 2 a la 17, donde el primer certificado criptográfico valida que $K_{BLOB\ priv}$ es efímero y que $K_{BLOB\ priv}$ no puede salir del segundo contexto de seguridad (7).

19. Un medio portador que comprende un código legible por ordenador configurado para hacer que un ordenador lleve a cabo el método de cualquiera de las reivindicaciones anteriores.

20. Un dispositivo criptográfico que comprende un primer contexto de seguridad (5), el primer contexto de seguridad (5) comprendiendo:

un primer transceptor (13) configurado para recibir una primera clave pública $K_{BLOB\ pub}$ y un primer certificado criptográfico, comprendiendo información a partir de la cual puede validarse el origen de la primera clave pública $K_{BLOB\ pub}$, de un segundo contexto de seguridad (7);

un primer procesador (17) configurado para llevar a cabo operaciones criptográficas, el primer procesador (17) estando configurado para:

generar una lista de control de acceso que corresponde a los datos a ser transferidos, donde la lista de control de acceso especifica que debe presentarse una credencial de uso válida para permitir un primer tipo de uso de los datos;

validar que la primera clave pública $K_{BLOB\ pub}$ se originó en el segundo contexto de seguridad (7);

cifrar los datos y la lista de control de acceso correspondiente con la primera clave pública $K_{BLOB\ pub}$;

donde el primer transceptor (13) está configurado para enviar los datos y lista de control de acceso correspondiente cifrados, e información a partir de la cual el origen de los datos puede validarse, al segundo contexto de seguridad (7).

21. Un dispositivo criptográfico que comprende un segundo contexto de seguridad (7), para la cooperación con un dispositivo o dispositivos que comprenden un primer contexto de seguridad (5), el dispositivo criptográfico comprendiendo:

un procesador (19), configurado para llevar a cabo operaciones criptográficas, el procesador (19) estando configurado para:

generar un primer par de claves criptográficas y un primer certificado criptográfico, comprendiendo el primer par de claves criptográficas una primera clave pública, $K_{BLOB\ pub}$, y una primera clave privada, $K_{BLOB\ priv}$ y el primer certificado criptográfico comprendiendo información a partir de la cual el origen de la primera clave pública $K_{BLOB\ pub}$ puede ser validado;

un transceptor (15), configurado para:

enviar la primera clave pública $K_{BLOB\ pub}$ y el primer certificado criptográfico al primer contexto de seguridad (5); y

recibir los datos cifrados y una lista de control de acceso correspondiente, e información a partir de la cual el origen de los datos puede validarse desde el primer contexto de seguridad (5);

el procesador (19) configurado además para:

validar el origen de los datos;

descifrar los datos y la lista de control de acceso correspondiente cifrados utilizando la primera clave privada $K_{BLOB\ priv}$.

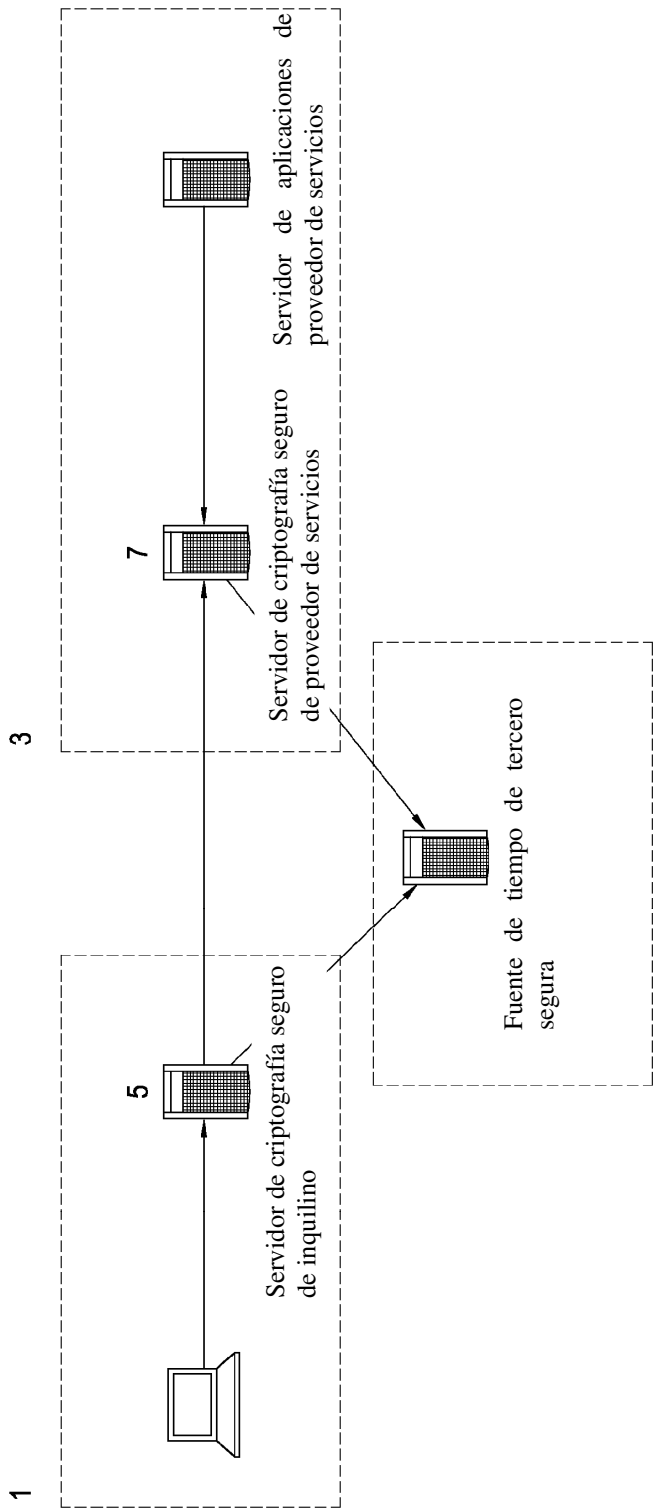
1
2
3
5
7
Servidor de criptografía seguro de inquilino
Fuente de tiempo de tercero segura
Servidor de criptografía seguro de proveedor de servicios
Servidor de aplicaciones de proveedor de servicios

Figura 1(a)

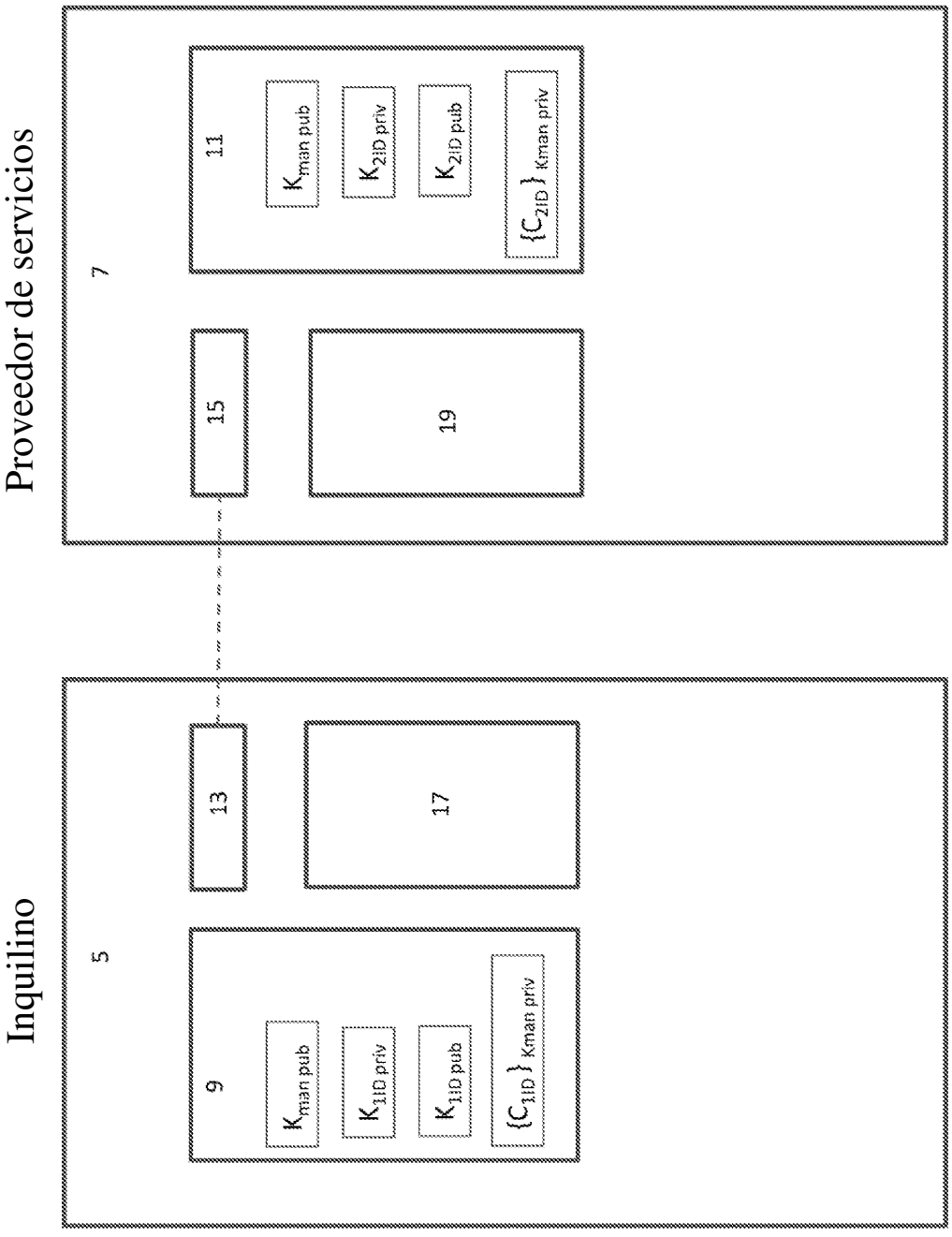
Proveedor de servicios
7
11
$K_{man\ pub}$
$K_{2ID\ priv}$
$K_{2ID\ pub}$
$\{C_{2ID}\}_{Kman\ priv}$
15
19
Inquilino
5
13
17
9
$K_{man\ pub}$
$K_{1ID\ priv}$
$K_{1ID\ pub}$
$\{C_{1ID}\}_{Kman\ priv}$

Figura 1(b)

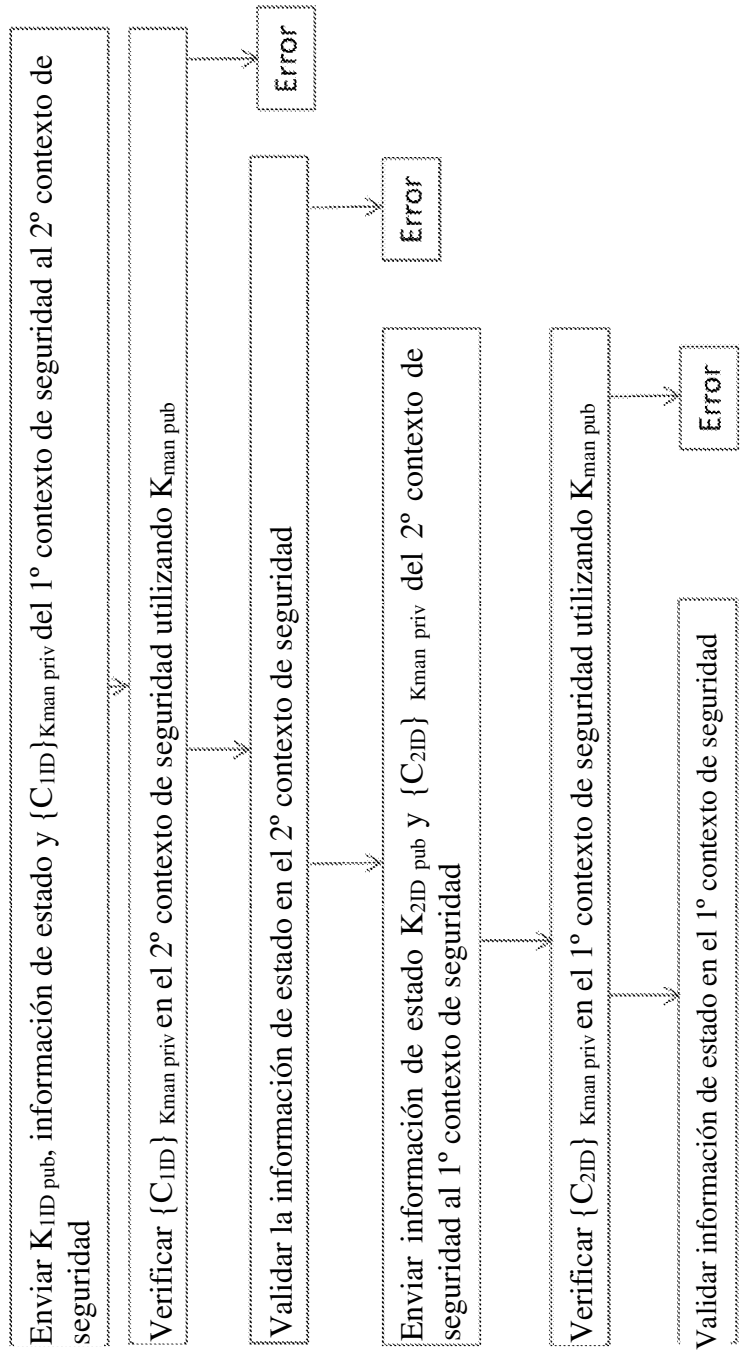
S201
Enviar $K_{1ID\ pub}$, información de estado y $\{C_{1ID}\}_{Kman\ priv}$ del 1º contexto de seguridad al 2º contexto de seguridad
S202
Verificar $\{C_{1ID}\}_{Kman\ priv}$ en el 2º contexto de seguridad utilizando $K_{man\ pub}$
Error
S203
Validar la información de estado en el 2º contexto de seguridad
Error
S204
Enviar información de estado $K_{2ID\ pub}$ y $\{C_{2ID}\}_{Kman\ priv}$ del 2º contexto de seguridad al 1º contexto de seguridad
S205
Verificar $\{C_{2ID}\}_{Kman\ priv}$ en el 1º contexto de seguridad utilizando $K_{man\ pub}$
Error
S206
Validar información de estado en el 1º contexto de seguridad

Figura 2(a)

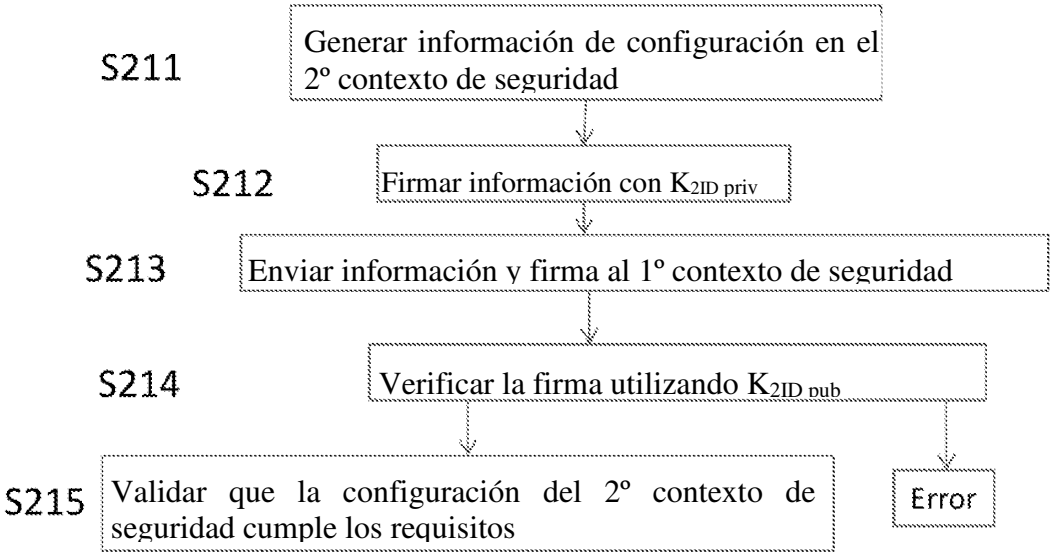
S211
Generar información de configuración en el 2º contexto de seguridad
S212
Firmar información con $K_{2ID\ priv}$
S213
Enviar información y firma al 1º contexto de seguridad
S214
Verificar la firma utilizando $K_{2ID\ pub}$
S215
Validar que la configuración del 2º contexto de seguridad cumple los requisitos
Error

Figura 2(b)

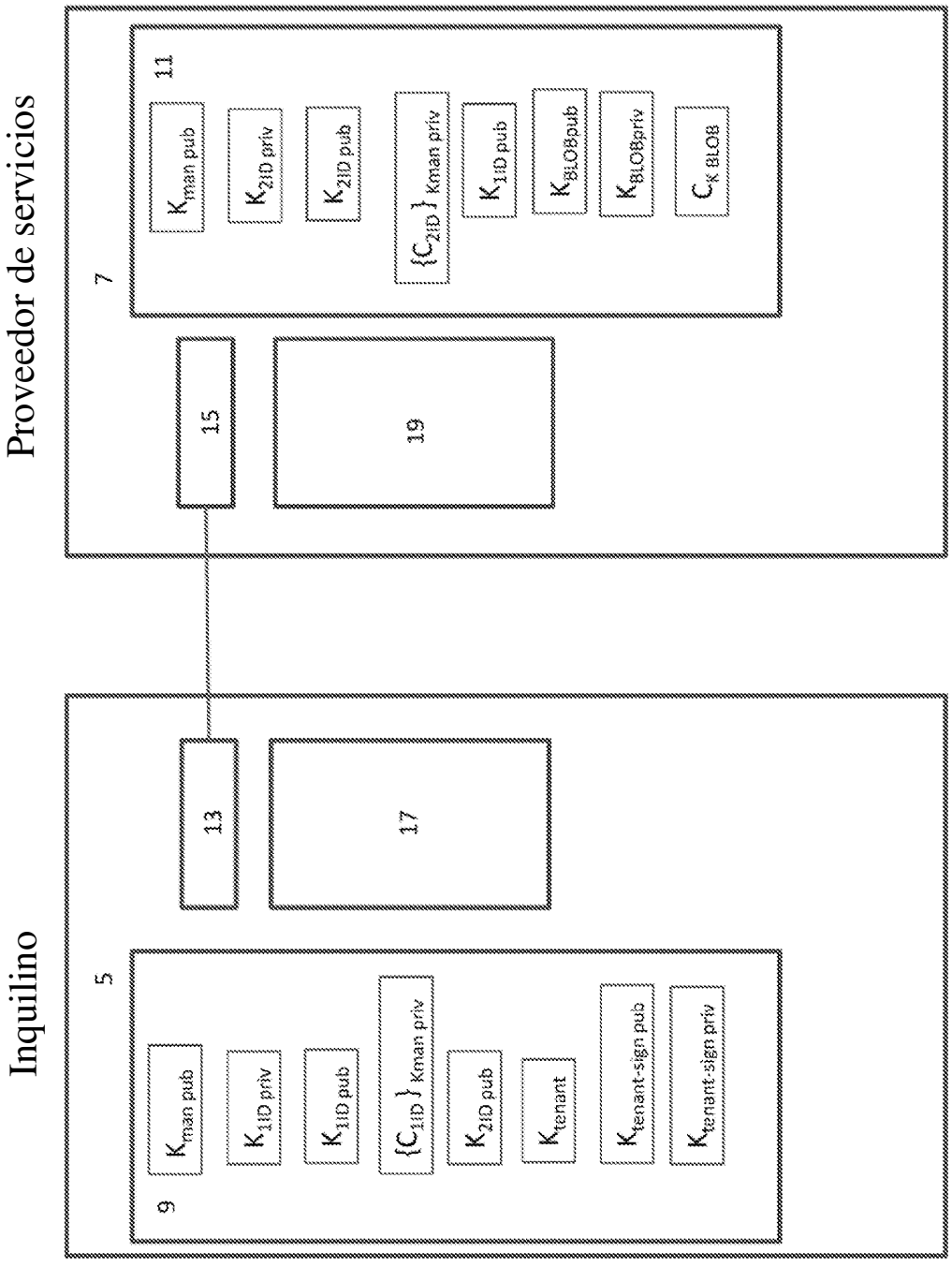
Proveedor de servicios
7
11
$K_{man\ pub}$
$K_{21D\ priv}$
$K_{21D\ pub}$
$\{C_{21D}\}_{Kman\ priv}$
$K_{11D\ pub}$
$K_{BLOBpub}$
$K_{BLOBpriv}$
$C_{K\ BLOB}$
15
19
Inquilino
5
9
$K_{man\ pub}$
$K_{11D\ priv}$
$K_{11D\ pub}$
$\{C_{11D}\}_{Kman\ priv}$
$K_{21D\ pub}$
K_{tenant}
$K_{tenant\text{-}sign\ pub}$
$K_{tenant\text{-}sign\ priv}$
13
17

Figura 3

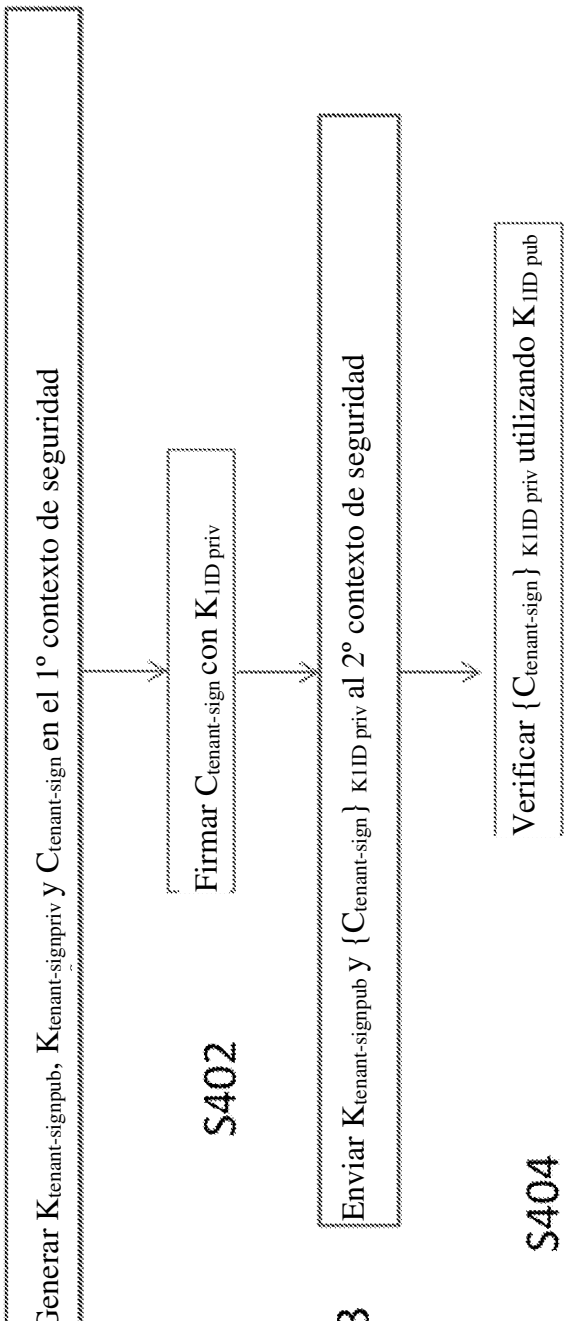
S401
Generar $K_{tenant-signpub}$, $K_{tenant-signpriv}$ y $C_{tenant-sign}$ en el 1º contexto de seguridad
S402
Firmar $C_{tenant-sign}$ con $K_{IID\ priv}$
S403
Enviar $K_{tenant-signpub}$ y $\{C_{tenant-sign}\}_{K1ID\ priv}$ al 2º contexto de seguridad
S404
Verificar $\{C_{tenant-sign}\}_{K1ID\ priv}$ utilizando $K_{IID\ pub}$

Figura 4(a)

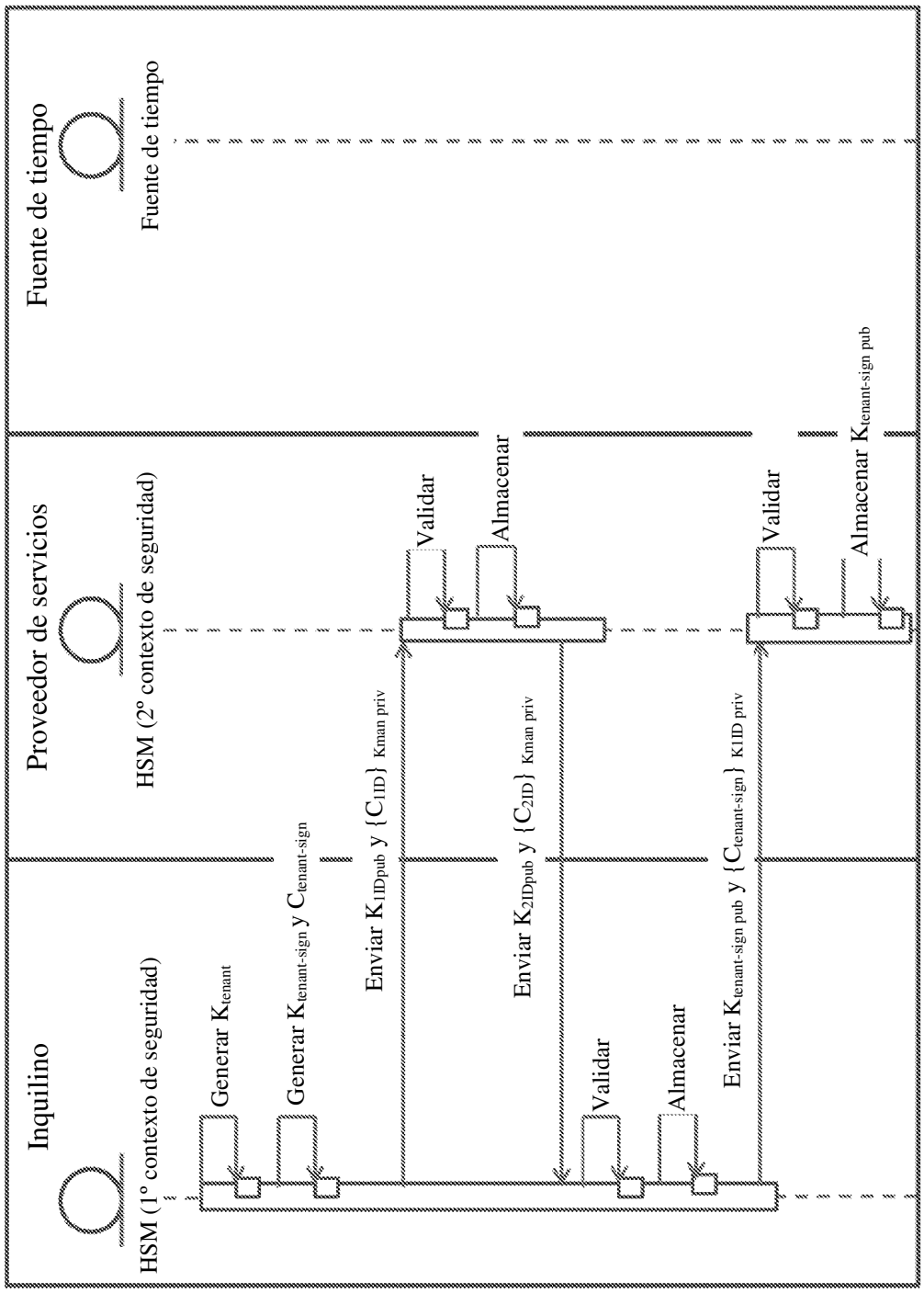
Inquilino
Proveedor de servicios
Fuente de tiempo
HSM (1º contexto de seguridad)
HSM (2º contexto de seguridad)
Fuente de tiempo
Generar K_{tenant}
Generar $K_{tenant-sign}$ y $C_{tenant-sign}$
Enviar K_{1IDpub} y $\{C_{1ID}\}_{Kman\ priv}$
Validar
Almacenar
Enviar K_{2IDpub} y $\{C_{2ID}\}_{Kman\ priv}$
Validar
Almacenar
Enviar $K_{tenant-sign\ pub}$ y $\{C_{tenant-sign}\}_{K1ID\ priv}$
Validar
Almacenar $K_{tenant-sign\ pub}$

Figura 4(b)

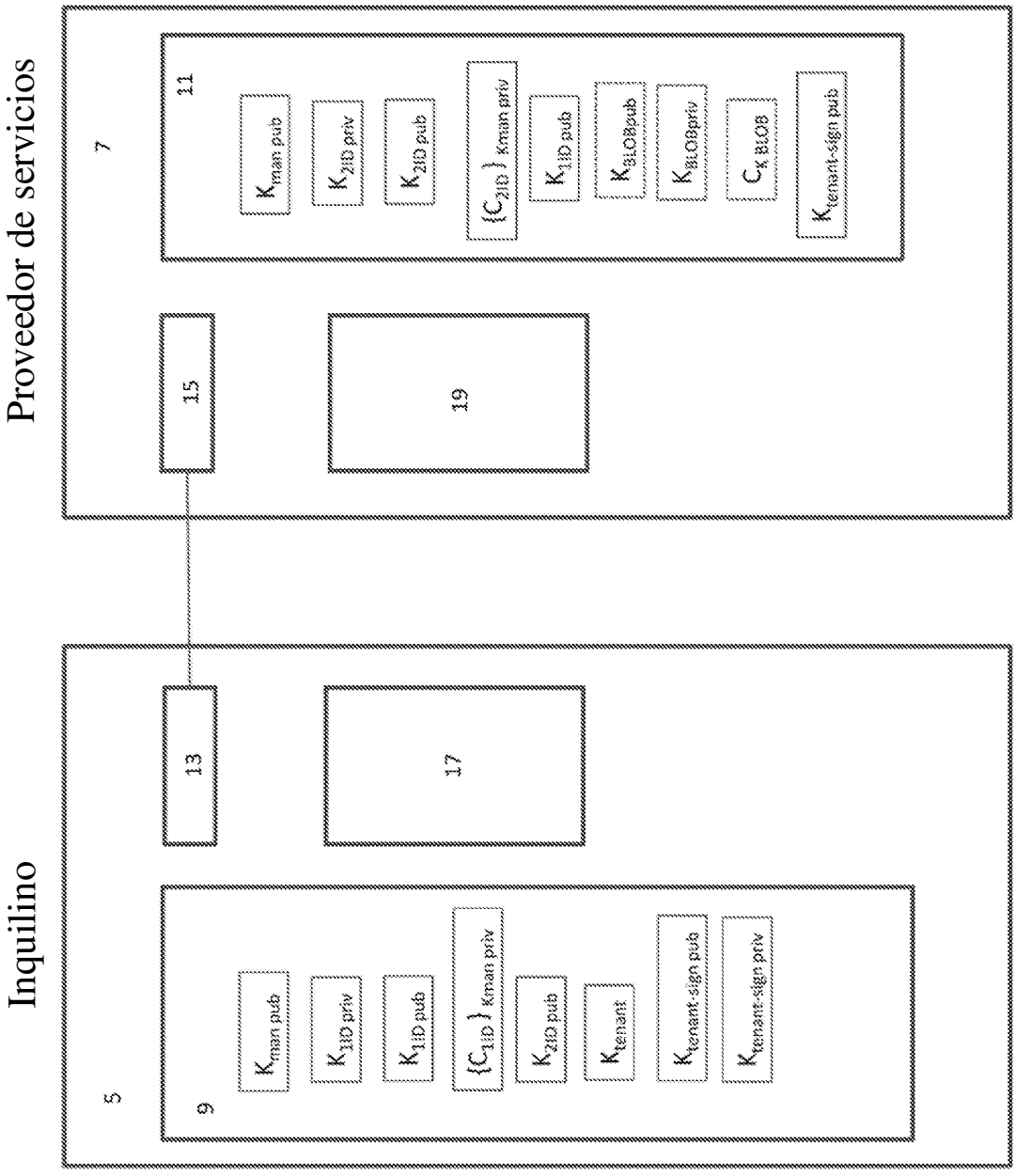
Proveedor de servicios
7
11
$K_{man\ pub}$
$K_{2ID\ priv}$
$K_{2ID\ pub}$
$\{C_{2ID}\}_{kman\ priv}$
$K_{1ID\ pub}$
$K_{BLOBpub}$
$K_{BLOBpriv}$
$C_{K\ BLOB}$
$K_{tenant\text{-}sign\ pub}$
15
19
Inquilino
5
9
$K_{man\ pub}$
$K_{1ID\ priv}$
$K_{1ID\ pub}$
$\{C_{1ID}\}_{kman\ priv}$
$K_{2ID\ pub}$
K_{tenant}
$K_{tenant\text{-}sign\ pub}$
$K_{tenant\text{-}sign\ priv}$
13
17

Figura 5

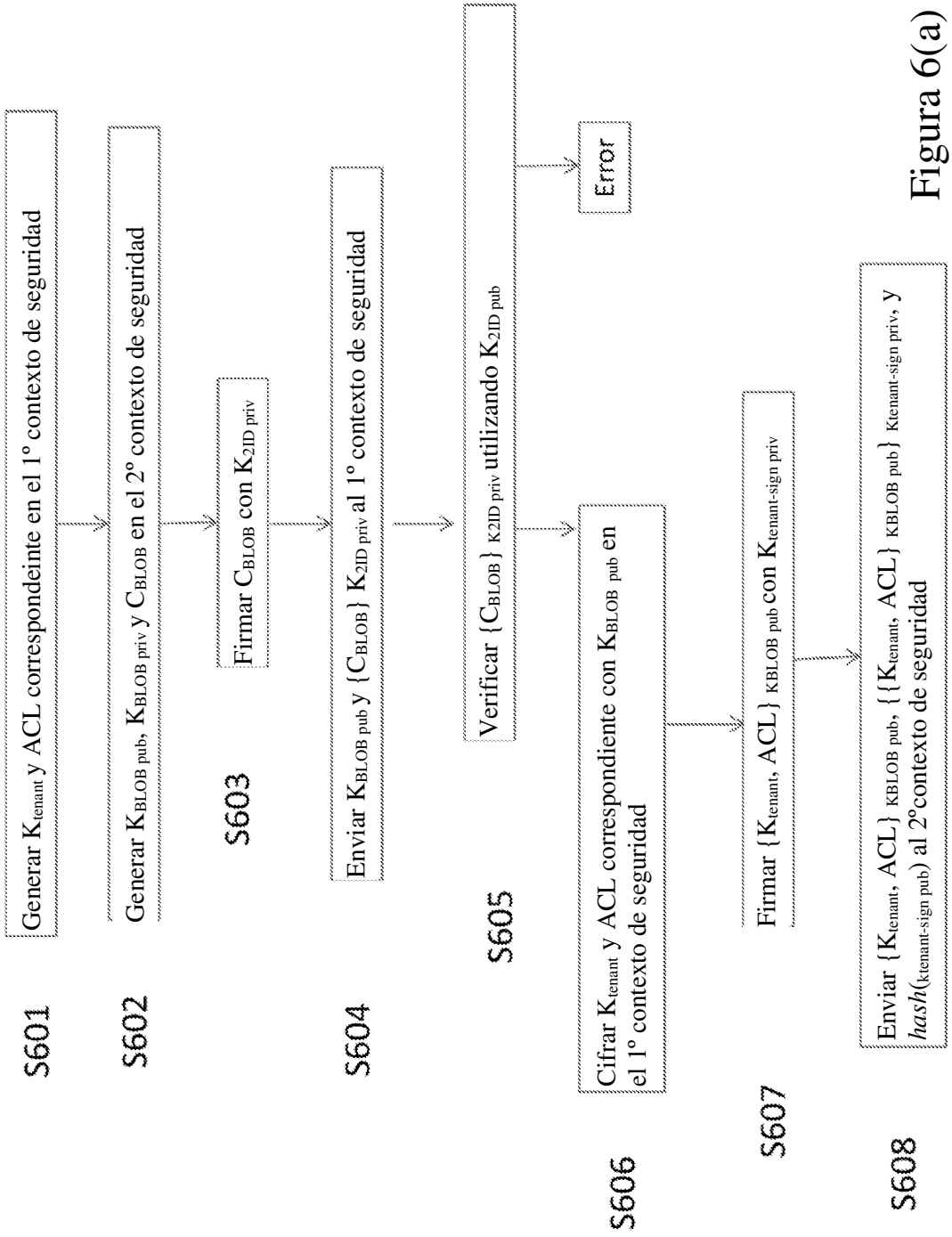
S601
Generar K_{tenant} y ACL correspondeinte en el 1º contexto de seguridad
S602
Generar $K_{BLOB\ pub}$, $K_{BLOB\ priv}$ y C_{BLOB} en el 2º contexto de seguridad
S603
Firmar C_{BLOB} con $K_{2ID\ priv}$
S604
Enviar $K_{BLOB\ pub}$ y {C_{BLOB}} $K_{2ID\ priv}$ al 1º contexto de seguridad
S605
Verificar {C_{BLOB}} $K2ID_{priv}$ utilizando $K_{2ID\ pub}$
Error
S606
Cifrar K_{tenant} y ACL correspondiente con $K_{BLOB\ pub}$ en el 1º contexto de seguridad
S607
Firmar {K_{tenant}, ACL} $K_{BLOB\ pub}$ con $K_{tenant\text{-}sign\ priv}$
S608
Enviar {K_{tenant}, ACL} $K_{BLOB\ pub}$, {{K_{tenant}, ACL} $K_{BLOB\ pub}$} $K_{tenant\text{-}sign\ priv}$, y $hash_{(ktenant\text{-}sign\ pub)}$ al 2ºcontexto de seguridad

Figura 6(a)

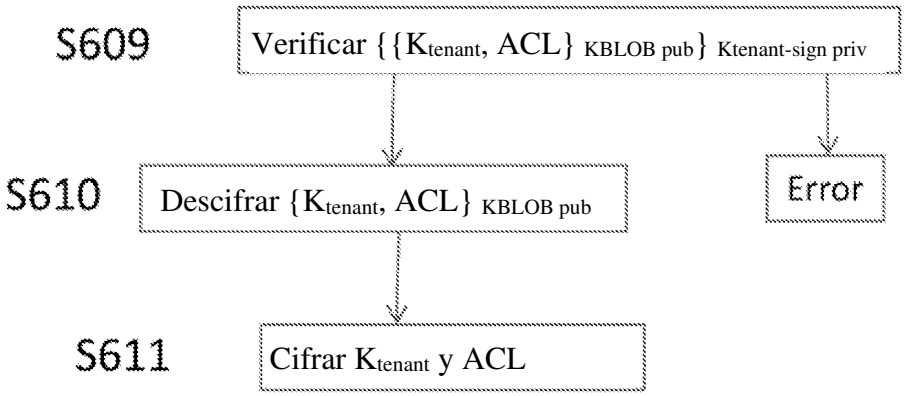
S609
Verificar {{Ktenant, ACL} KBLOB pub} Ktenant-sign priv
S610
Descifrar {Ktenant, ACL} KBLOB pub
Error
S611
Cifrar Ktenant y ACL

Figura 6(b)

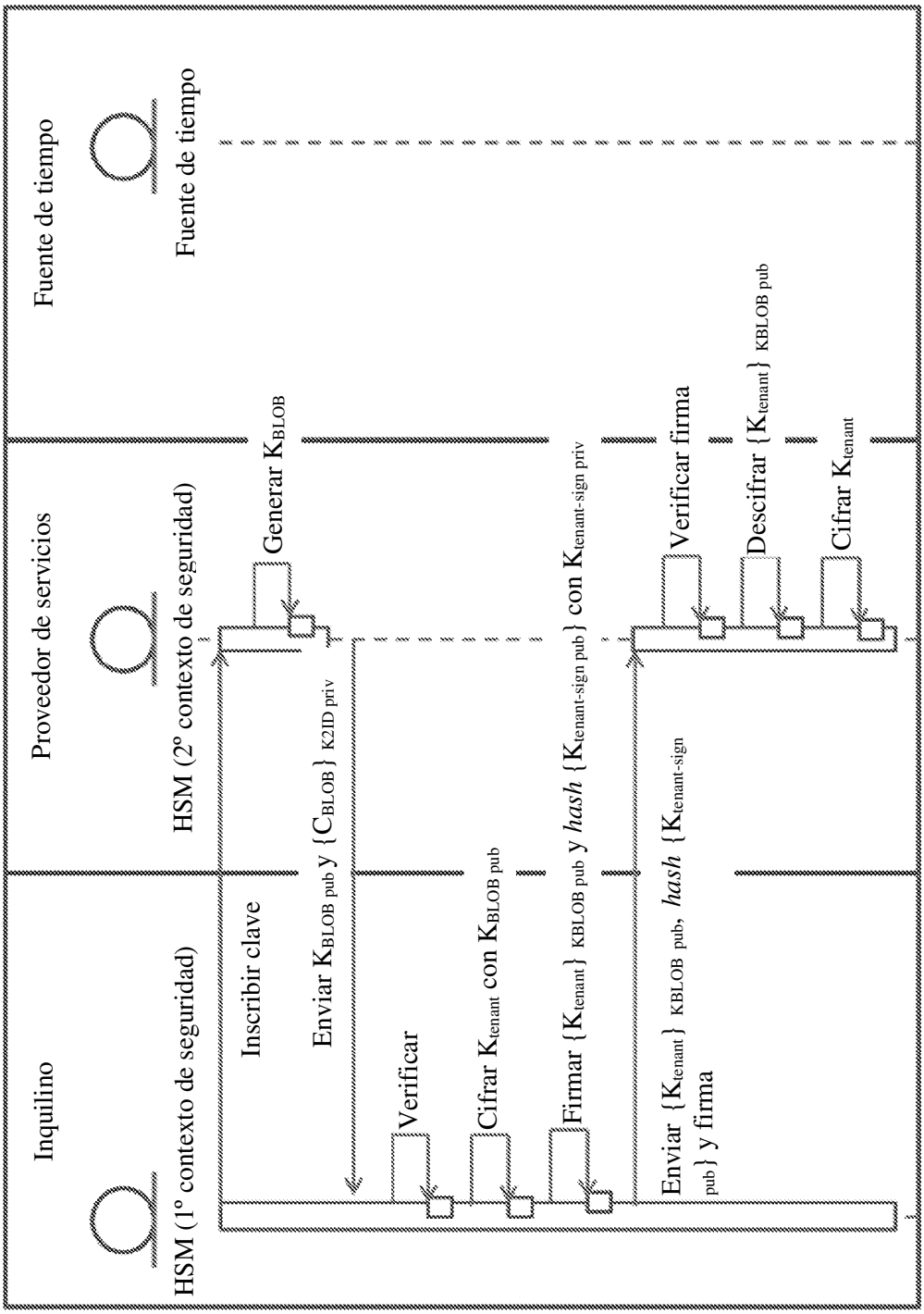
Inquilino
Proveedor de servicios
Fuente de tiempo
HSM (1º contexto de seguridad)
HSM (2º contexto de seguridad)
Fuente de tiempo
Inscribir clave
Generar K_{BLOB}
Enviar $K_{BLOB\ pub}$ y $\{C_{BLOB}\}_{K2ID\ priv}$
Verificar
Cifrar K_{tenant} con $K_{BLOB\ pub}$
Firmar $\{K_{tenant}\}_{KBLOB\ pub}$ y *hash* $\{K_{tenant\text{-}sign\ pub}\}$ con $K_{tenant\text{-}sign\ priv}$
Enviar $\{K_{tenant}\}_{KBLOB\ pub}$, *hash* $\{K_{tenant\text{-}sign\ pub}\}$ y firma
Verificar firma
Descifrar $\{K_{tenant}\}_{KBLOB\ pub}$
Cifrar K_{tenant}

Figura 7(a)

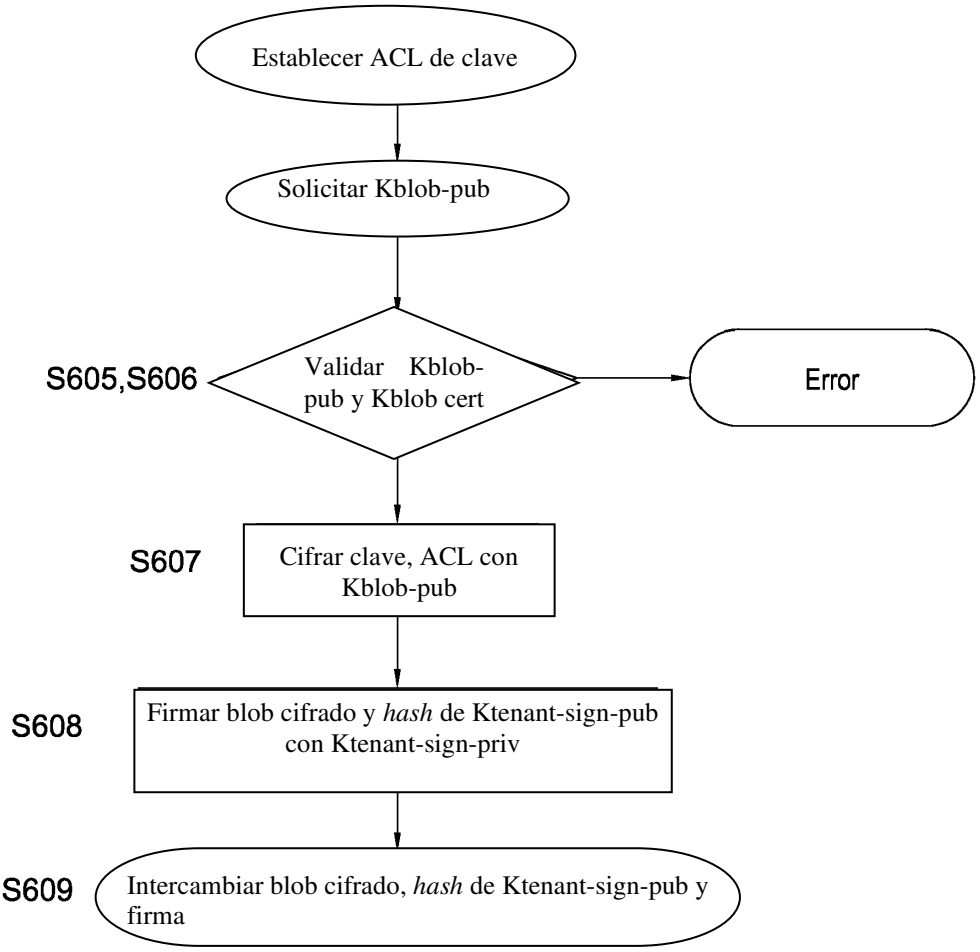
Establecer ACL de clave
Solicitar Kblob-pub
S605,S606
Validar Kblob-pub y Kblob cert
Error
S607
Cifrar clave, ACL con Kblob-pub
S608
Firmar blob cifrado y *hash* de Ktenant-sign-pub con Ktenant-sign-priv
S609
Intercambiar blob cifrado, *hash* de Ktenant-sign-pub y firma

Figura 7(b)

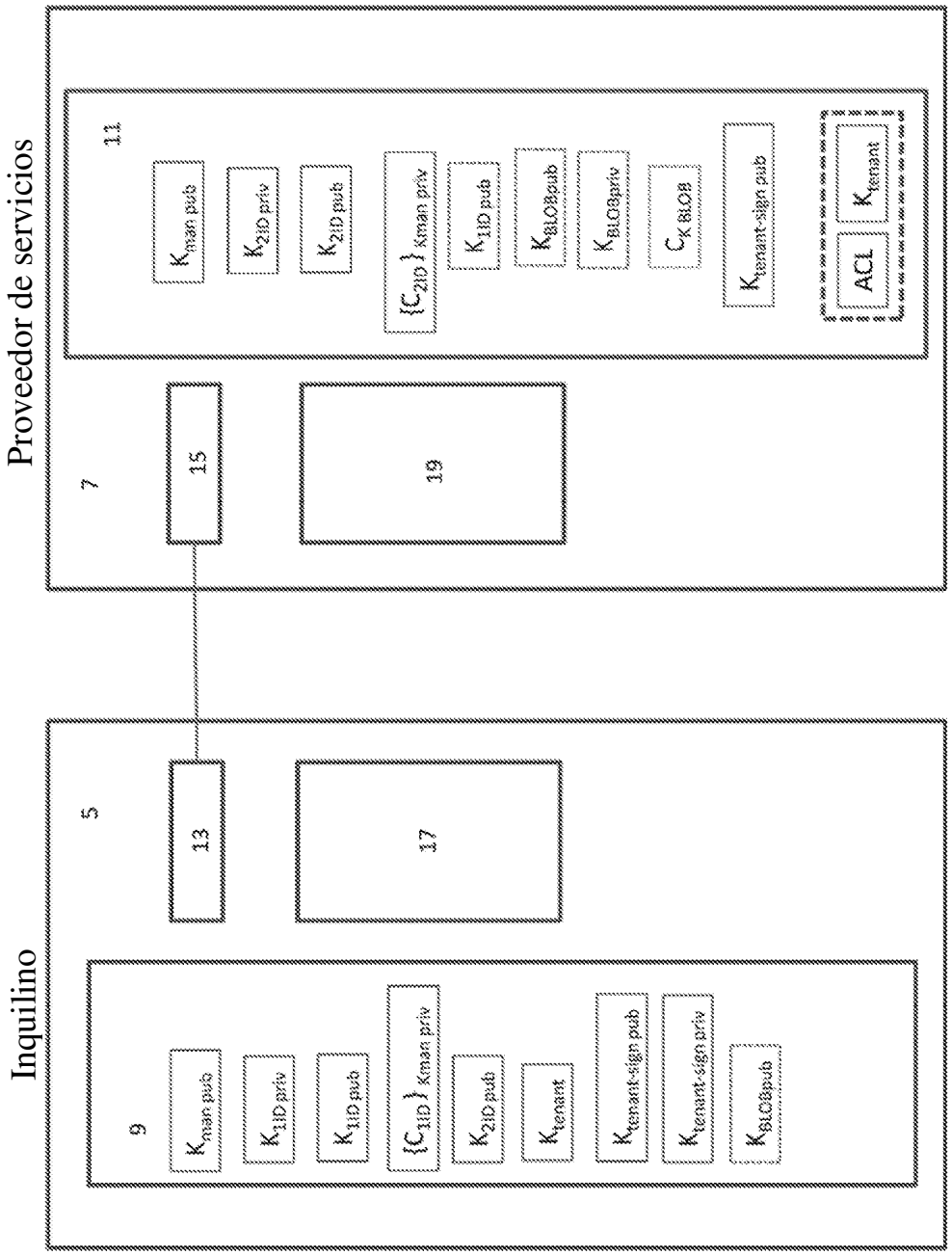
Proveedor de servicios
7
11
$K_{man\ pub}$
$K_{2ID\ priv}$
$K_{2ID\ pub}$
$\{C_{2ID}\}_{K man\ priv}$
$K_{1ID\ pub}$
$K_{BLOBpub}$
$K_{BLOBpriv}$
$C_{K\ BLOB}$
$K_{tenant\text{-}sign\ pub}$
ACL
K_{tenant}
15
19
Inquilino
5
9
$K_{man\ pub}$
$K_{1ID\ priv}$
$K_{1ID\ pub}$
$\{C_{1ID}\}_{K man\ priv}$
$K_{2ID\ pub}$
K_{tenant}
$K_{tenant\text{-}sign\ pub}$
$K_{tenant\text{-}sign\ priv}$
$K_{BLOBpub}$
13
17

Figura 8(a)

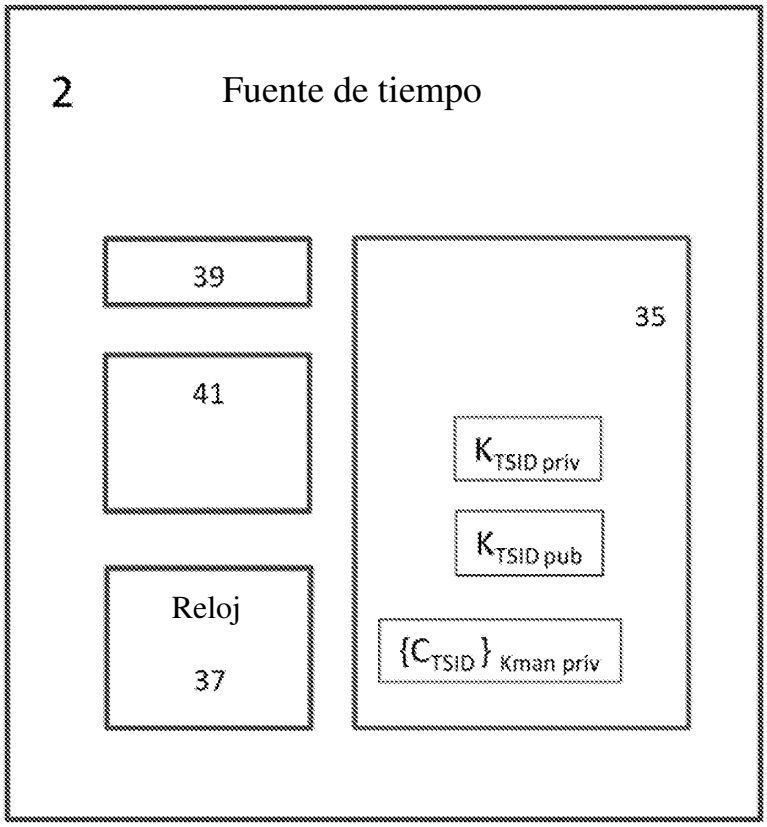
2
Fuente de tiempo
39
41
Reloj
37
35
$K_{TSID\ priv}$
$K_{TSID\ pub}$
$\{C_{TSID}\}_{Kman\ priv}$

Figura 8(b)

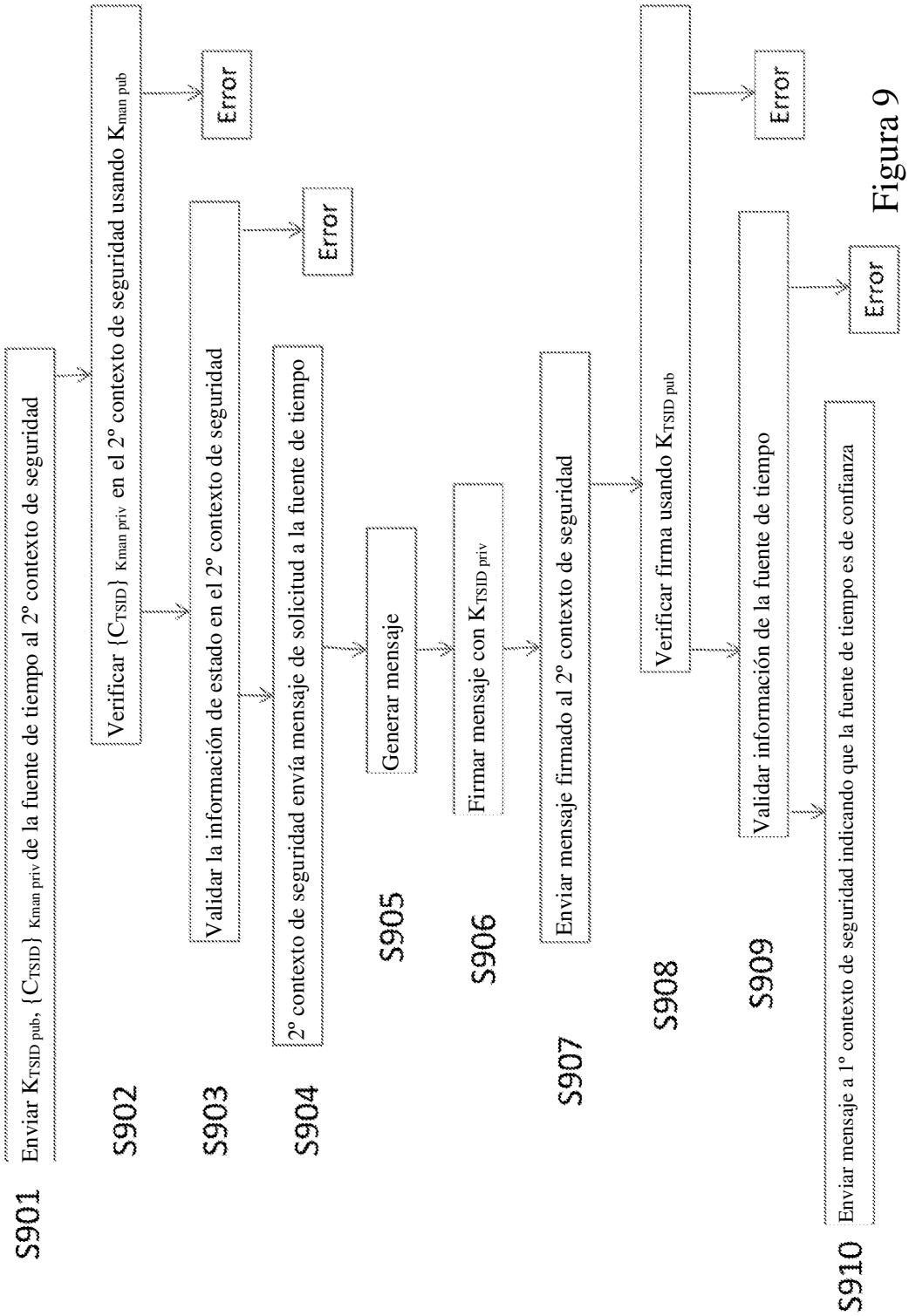
S901
Enviar $K_{TSID\ pub}$, $\{C_{TSID}\}_{Kman\ priv}$ de la fuente de tiempo al 2º contexto de seguridad
S902
Verificar $\{C_{TSID}\}_{Kman\ priv}$ en el 2º contexto de seguridad usando $K_{man\ pub}$
Error
S903
Validar la información de estado en el 2º contexto de seguridad
Error
S904
2º contexto de seguridad envía mensaje de solicitud a la fuente de tiempo
S905
Generar mensaje
S906
Firmar mensaje con $K_{TSID\ priv}$
S907
Enviar mensaje firmado al 2º contexto de seguridad
S908
Verificar firma usando $K_{TSID\ pub}$
Error
S909
Validar información de la fuente de tiempo
Error
S910
Enviar mensaje a 1º contexto de seguridad indicando que la fuente de tiempo es de confianza

Figura 9

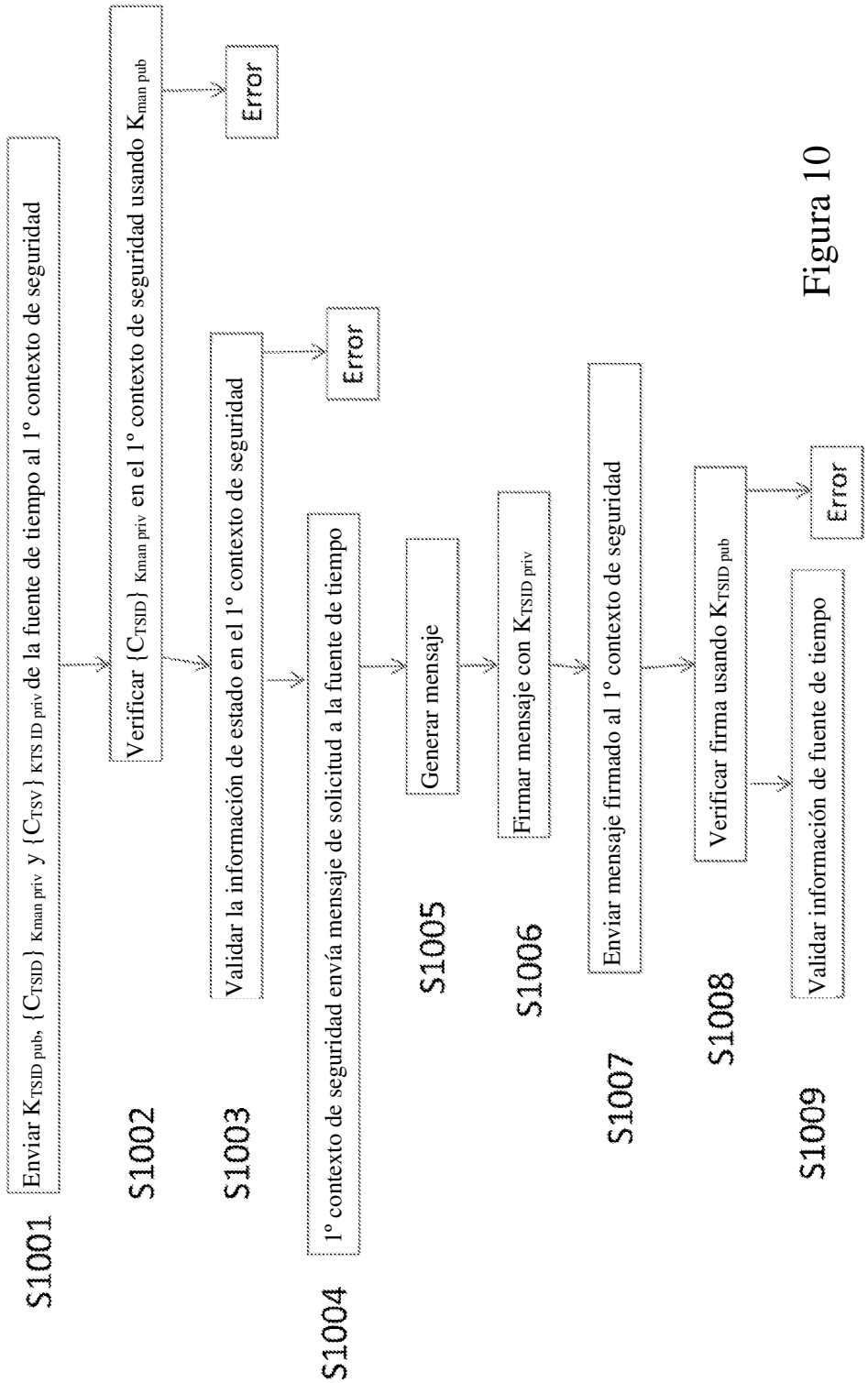
S1001
Enviar $K_{TSID\ pub}$, $\{C_{TSID}\}_{Kman\ priv}$ y $\{C_{TSV}\}_{KTS\ ID\ priv}$ de la fuente de tiempo al 1° contexto de seguridad
S1002
Verificar $\{C_{TSID}\}_{Kman\ priv}$ en el 1° contexto de seguridad usando $K_{man\ pub}$
Error
S1003
Validar la información de estado en el 1° contexto de seguridad
Error
S1004
1° contexto de seguridad envía mensaje de solicitud a la fuente de tiempo
S1005
Generar mensaje
S1006
Firmar mensaje con $K_{TSID\ priv}$
S1007
Enviar mensaje firmado al 1° contexto de seguridad
S1008
Verificar firma usando $K_{TSID\ pub}$
Error
S1009
Validar información de fuente de tiempo

Figura 10

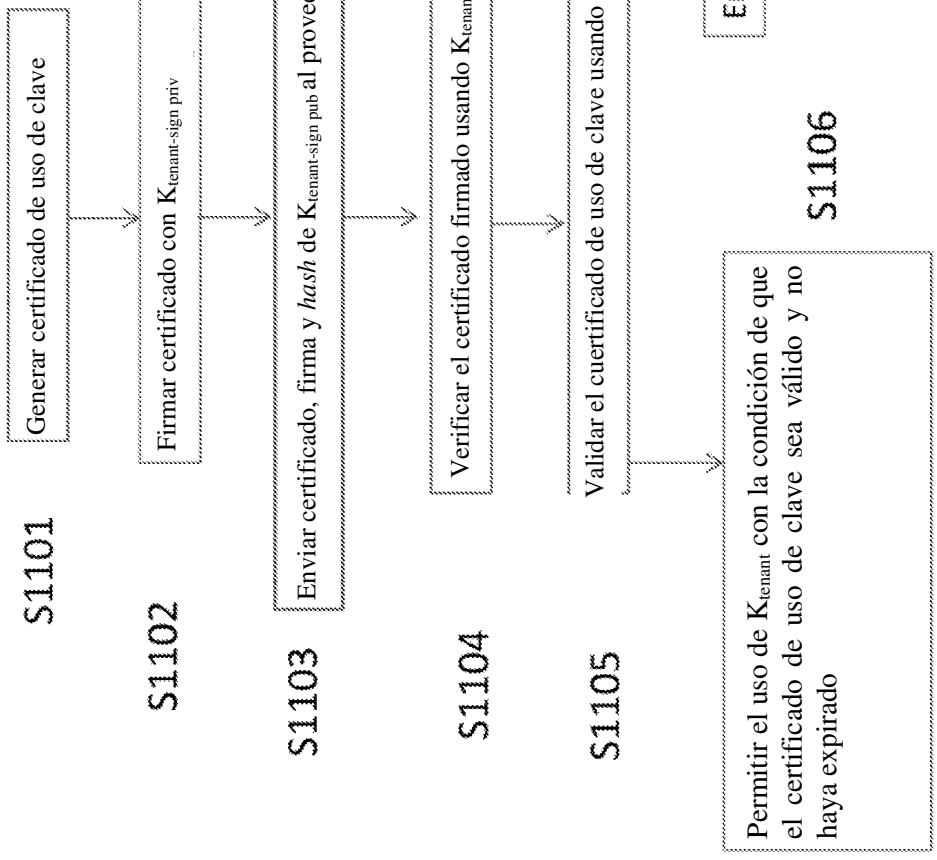
S1101
Generar certificado de uso de clave
S1102
Firmar certificado con $K_{tenant\text{-}sign\ priv}$
S1103
Enviar certificado, firma y *hash* de $K_{tenant\text{-}sign\ pub}$ al proveedor de servicios
S1104
Verificar el certificado firmado usando $K_{tenant\text{-}sign\ pub}$ en el 2º contexto de seguridad
Error
S1105
Validar el cuertificado de uso de clave usando ACL
Error
S1106
Permitir el uso de K_{tenant} con la condición de que el certificado de uso de clave sea válido y no haya expirado

Figura 11

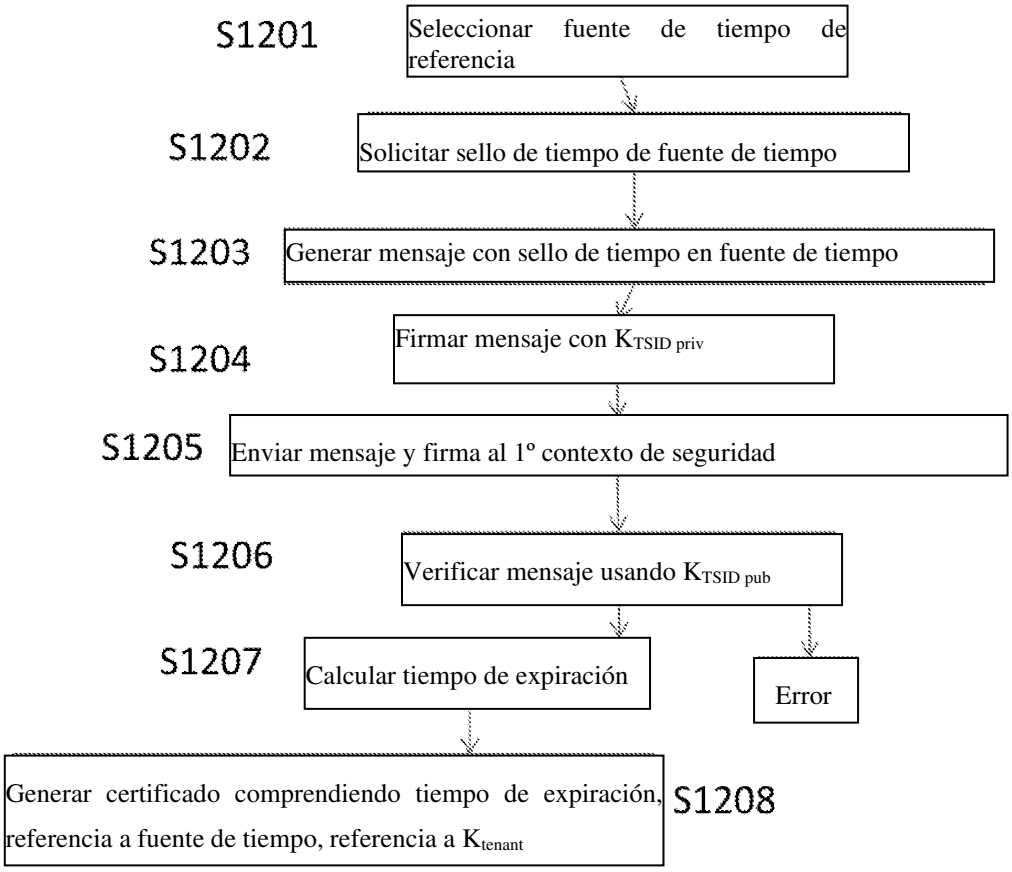
S1201
Seleccionar fuente de tiempo de referencia
S1202
Solicitar sello de tiempo de fuente de tiempo
S1203
Generar mensaje con sello de tiempo en fuente de tiempo
S1204
Firmar mensaje con $K_{TSID\ priv}$
S1205
Enviar mensaje y firma al 1º contexto de seguridad
S1206
Verificar mensaje usando $K_{TSID\ pub}$
S1207
Calcular tiempo de expiración
Error
Generar certificado comprendiendo tiempo de expiración, referencia a fuente de tiempo, referencia a K_{tenant}
S1208

Figura 12

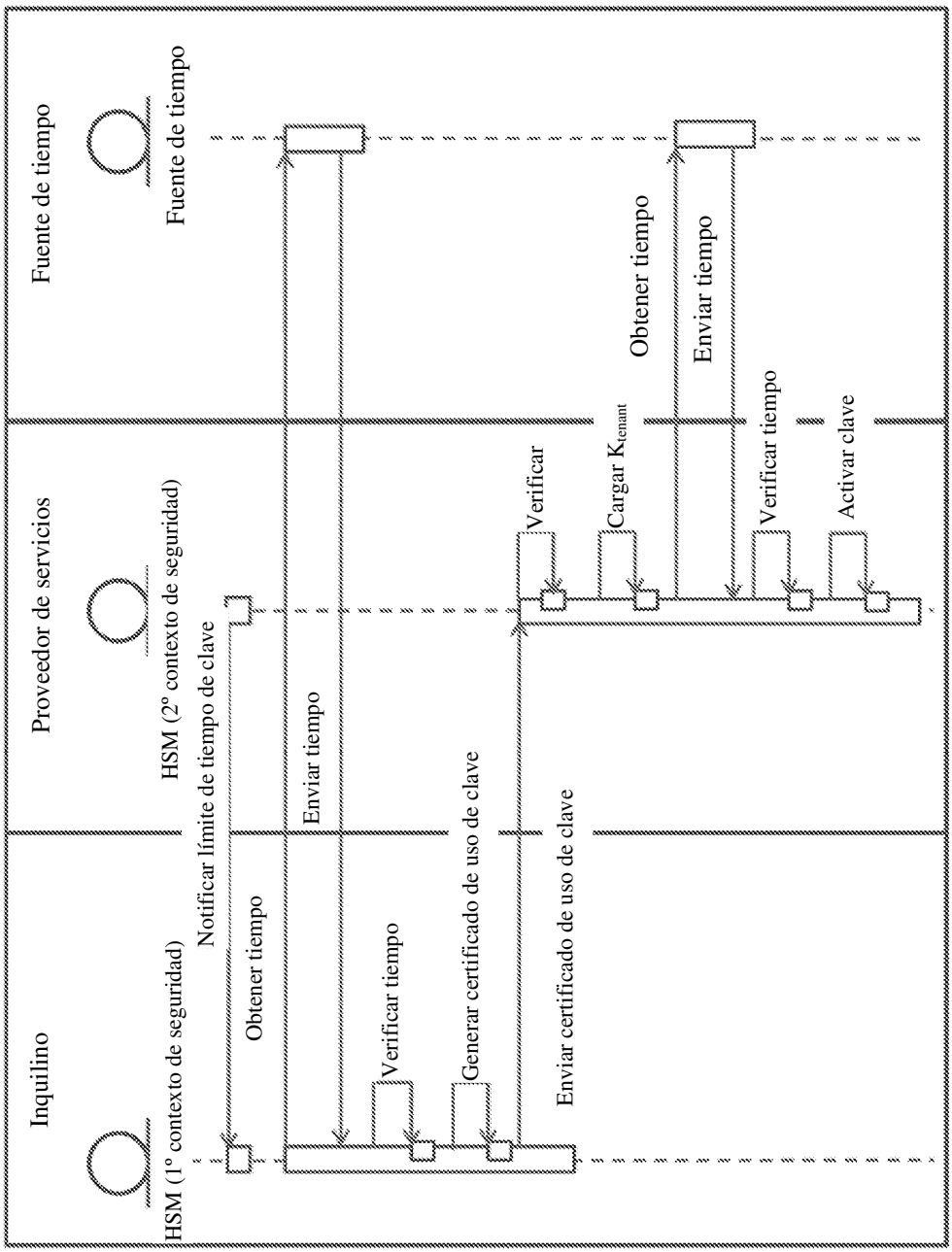
Inquilino
Proveedor de servicios
Fuente de tiempo
HSM (1º contexto de seguridad)
HSM (2º contexto de seguridad)
Fuente de tiempo
Notificar límite de tiempo de clave
Obtener tiempo
Enviar tiempo
Verificar tiempo
Generar certificado de uso de clave
Verificar
Enviar certificado de uso de clave
Cargar K_{tenant}
Obtener tiempo
Enviar tiempo
Verificar tiempo
Activar clave

Figura 13

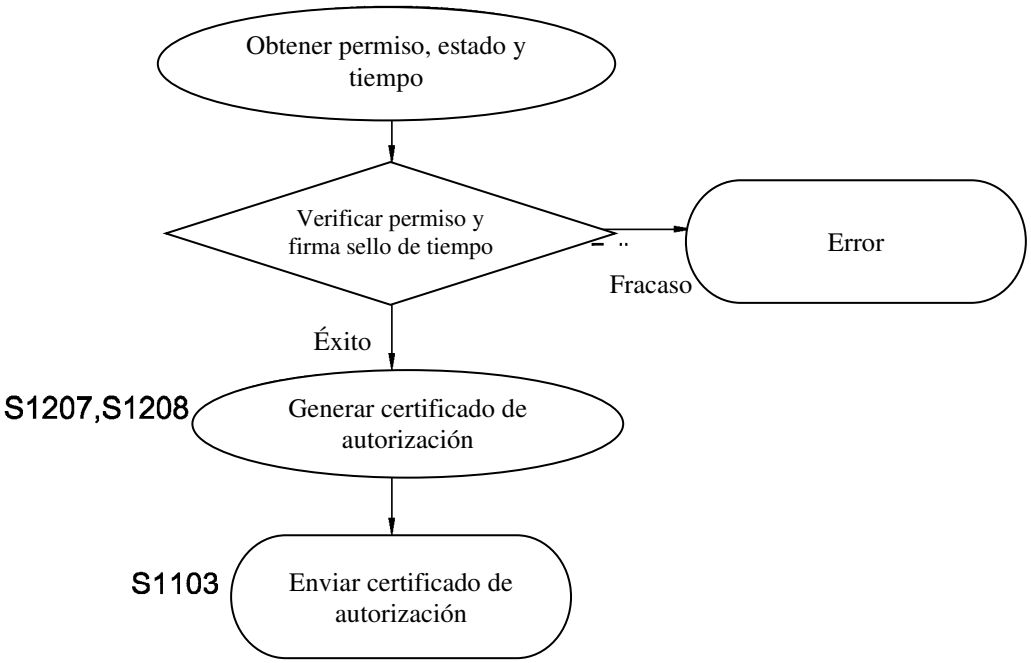
Obtener permiso, estado y tiempo
Verificar permiso y firma sello de tiempo
Fracaso
Error
Éxito
S1207,S1208
Generar certificado de autorización
S1103
Enviar certificado de autorización

Figura 14