(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 769 091**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/00 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.11.2016 PCT/EP2016/077356**

(87) Fecha y número de publicación internacional: **18.05.2017 WO17081208**

(96) Fecha de presentación y número de la solicitud europea: **10.11.2016 E 16794342 (2)**

(97) Fecha y número de publicación de la concesión europea: **01.01.2020 EP 3375133**

(54) Título: **Procedimiento de securización y de autentificación de una telecomunicación**

(30) Prioridad:

13.11.2015 FR 1560916

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.06.2020

(73) Titular/es:

AIRBUS CYBERSECURITY SAS (100.0%)
1 Boulevard Jean Moulin, ZAC de la Clef Saint Pierre
78990 Elancourt, FR

(72) Inventor/es:

BRUN, PAUL-EMMANUEL;
COHEN, RAPHAËL y
PETESQUE, NICOLAS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de securización y de autentificación de una telecomunicación

Campo

El campo de la invención se refiere a la securización de comunicaciones entre dos entidades comunicantes, tales como un cliente y un servidor que tienen interfaces de red. Más particularmente, la invención está relacionada con las comunicaciones securizadas que no necesitan una gestión de estados o el establecimiento de una sesión de comunicación que se desea securizar. Finalmente, el campo de la invención se refiere a las telecomunicaciones que comprenden una autentificación que permite el establecimiento de comunicaciones securizadas ad hoc las cuales ofrecen una flexibilidad de arquitectura limitando el uso de un tercero de autentificación.

Estado de la técnica

En el campo de los servicios *web*, el estilo de arquitectura de *software* de tipo REST, cuyo acrónimo designa "Representational State Transfer", se ha extendido ampliamente debido a su simplicidad de puesta en práctica y de integración en sistemas distribuidos. En una aplicación *web* que se basa en una arquitectura de tipo REST, una estación de cliente hace uso de recursos distribuidos en una o varias estaciones de servidor con la ayuda de peticiones utilizando, por ejemplo, el protocolo http, cuyo acrónimo designa "Hypertext Transfer Protocol", y haciendo referencia a un URI, cuyo significado es "Uniform Resource Identifier", que representa la dirección única del recurso en la red. Como respuesta a esta petición, el servidor reenvía a la estación de cliente los recursos solicitados, generalmente en el formato XML ó JSON. Una de las características esenciales de la arquitectura REST es la de prohibir, en el nivel del servidor, todo contexto de comunicación con la estación de cliente más allá del espacio de tiempo de recepción de la petición. Este modo de comunicación sin estados, conocido también con la denominación anglosajona "stateless", garantiza, en la estación de servidor, una escalabilidad. En efecto, este último, tras la recepción de la petición, puede liberar inmediatamente sus recursos necesarios para la comunicación con la estación de cliente, dejándolos, así, disponibles para una nueva comunicación y evitando la sobrecarga de estos recursos del sistema.

En el campo de la securización de las telecomunicaciones existen diferentes técnicas. Todas se basan en un mecanismo de autentificación que permite securizar intercambios entre dos entidades comunicantes.

Entre las soluciones que no implican la puesta en práctica de una sesión entre las dos entidades, se han extendido dos métodos de autentificación. Entre estos métodos, todos conllevan el intercambio de por lo menos un secreto entre el servidor y un cliente. El secreto puede adoptar la forma de una contraseña o de una clave. En lo sucesivo en la descripción, designaremos con el vocablo secreto ambos casos.

Un primer método de autentificación se basa en el intercambio de una clave API, es decir de un secreto compartido entre dos entidades comunicantes. En este caso, generalmente se define un secreto, tal como una contraseña, en el lado del servidor, y el mismo se transmite mediante la petición con destino a un cliente. A continuación, esta contraseña se intercambia en cada emisión de petición entre las entidades comunicantes.

Un problema de esta solución es que una interceptación de la petición permite que un tercero recupere el secreto compartido y que acceda más adelante al servidor de datos. Uno de los riesgos es que el acceso al servidor sea usurpado por un tercero no autorizado el cual puede, entonces, compartir datos sensibles.

Un segundo método de autentificación se basa en el establecimiento de una firma de clave API. Se comparte, entonces, inicialmente, un secreto entre dos entidades comunicantes, por ejemplo, mediante una fase de inscripción entre las dos entidades. A continuación, los secretos se almacenan en el lado del cliente y en el lado del servidor. El secreto es utilizado, entonces, para firmar los mensajes que son emitidos a continuación. Una de las ventajas es que el secreto no se comparte sistemáticamente durante la transmisión de cada mensaje entre dos entidades comunicantes. Esta solución limita las posibilidades de interceptación del secreto. La firma permite autentificar los mensajes una vez recibidos con el secreto que está almacenado en la entidad comunicante, pero que no se transfiere durante los intercambios.

Un problema de esta solución es que las contraseñas/secretos se deben almacenar en las entidades. Sin embargo, generalmente el almacenamiento del secreto se efectúa en texto claro, es decir de manera no cifrada. Uno de los peligros es que una usurpación de la base de datos del servidor por parte de un tercero permite acceder a los secretos de todos los clientes.

Entre las soluciones que implican la puesta en práctica de una sesión entre las dos entidades, se han extendido dos métodos de autentificación.

Un primer método se basa en la tecnología SAML que designa "Security Assertion Markup Language". Este método se basa en la definición de un tercero de autentificación tal como un servidor de autentificación. Esta solución implica la puesta en práctica de un sistema de gestión de claves PKI, acrónimo que designa "Public Key Infraestructure". Este método permite obtener una buena seguridad de los intercambios de datos entre las entidades comunicantes.

No obstante, resulta difícil de poner en práctica de manera simple ya que se debe parametrizar un tercero de autentificación. Además, es costoso y requiere el establecimiento de una sesión entre las entidades y/o los intercambios de certificados. Pro otra parte, en este método se utiliza generalmente el protocolo XML. Uno de los inconvenientes es que el encabezamiento de seguridad de este protocolo es muy prolijo y no está adaptado a comunicaciones de banda pasante reducida.

Una segunda solución se basa en el protocolo HTTPs el cual se basa también en un sistema de gestión de claves PKI y en el intercambio de certificados. Esta solución ofrece también una buena seguridad de los intercambios de datos entre entidades comunicantes. Por contra, esta solución es costosa y difícil de poner en práctica. Además, implica un mecanismo de intercambio de claves previo con un tercero de autentificación. Estos métodos se pueden desplegar en redes de banda ancha aunque, en redes más restringidas, pueden toparse con algunas limitaciones durante la puesta en práctica de los intercambios.

Además, uno de los problemas de un sistema de gestión de clave PKI es que, desde el punto de vista del servidor, resulta difícil, incluso imposible, suspender un equipo durante un espacio de tiempo determinado o indeterminado. Al poseer el tercero de autentificación derechos, resulta difícil disponer de una autonomía de gestión de las revocaciones o de las suspensiones de derechos desde el punto de vista del servidor de comunicación.

La patente US 8621598 B2 describe un mecanismo que se fundamenta en una arquitectura REST, por otro lado la solución impone la definición de un testigo de sesión que se transmite entre las entidades comunicantes. En esta solución, el testigo de autentificación es utilizado por el servidor para intercambios con un servidor de autentificación que autoriza o no la transferencia de datos entre el cliente y el servidor. Esta solución implica la puesta en práctica de un servidor de autentificación que comprende una base de datos en la cual se almacenan las claves privadas de los equipos de cliente.

Los siguientes documentos exponen procedimientos de autentificación securizada en el seno del protocolo DHCPv6:

Sheng Jiang, Sean Shen: "*Secure DHCPv6 Using CGAs*; draft-ietf-dhc-secure-dhcpv6-07.txt", *INTERNET ENGINEERING TASK FORCE* (IEFT); *DHC Working Group*; Update: RFC 3315, 14 septiembre de 2012;

R. Droms et al: "*Dynamic Host Configuration Protocol for IPv6 (DHCPv6*); draft-ietf-dhc-dhcpv6-27.txt",5. *INTERNET ENGINEERING TASK FORCE* (IETF); DHC *Working Group*, Internet Draft, 22 de octubre de 2003.

Existe una necesidad de definir un método de comunicación securizada para el intercambio de datos entre dos entidades comunicantes que sea sencillo de poner en práctica, que no se fundamente en un servidor de autentificación tercero y que no implique la definición, la puesta en práctica y la gestión de una sesión entre las entidades comunicantes.

Entre las necesidades de securización de dichos intercambios de datos, existe una necesidad de definir un método de comunicación que sea robusto a los ataques de tipo repetición, de tipo HDM, que designa un ataque del tipo "hombre en el medio" o incluso un ataque de tipo "eavesdropping", que designa un tipo de "escucha clandestina".

Resumen de la invención

La invención tiene como finalidad paliar los inconvenientes citados previamente.

La invención permite ofrecer un compromiso entre un nivel de seguridad suficiente para su puesta en práctica entre entidades comunicantes y una simplicidad de puesta en práctica de un cierto nivel de seguridad que permite intercambios sin estados entre dichas entidades. La invención permite prescindir de intercambios de certificados o del establecimiento de una sesión. Además, el procedimiento de la invención permite prescindir de un tercero de autentificación, tal como un servidor de autentificación.

Un objetivo de la invención se refiere a un procedimiento de comunicación entre dos entidades comunicantes, según la reivindicación independiente 1.

Una de las ventajas de la invención es permitir securizar un enlace de datos entre dos entidades comunicantes sin tener que implementar un tercero de autentificación, tal como un servidor de autentificación que almacena datos de autentificación de las entidades comunicantes. En el procedimiento de la invención, solamente las entidades comunicantes que intercambian datos ponen en práctica los mecanismos de seguridad del enlace de datos. Además, el procedimiento de la invención no requiere ninguna gestión de sesión o de estado entre las dos entidades comunicantes. Cada mensaje consta de los elementos de identificación, de autentificación y de seguridad que garantizan un enlace fiable.

Según un modo de realización, el conjunto de datos a firmar comprende una combinación de los siguientes datos:

- el identificador de mensaje;
- el identificador de usuario;

- una contraseña de una cuenta de usuario;
- el identificador del equipo;
- el perfil de seguridad;
- una información de encabezamientos o de un campo de datos de mensaje representativo del protocolo de transferencia de los datos útiles;
- los datos útiles.

Según un modo de realización, la primera entidad comunicante comprende una memoria para almacenar una clave pública de una segunda entidad comunicante, comprendiendo el perfil de seguridad:

- un primer parámetro que indica la presencia o no de un cifrado de los datos útiles efectuado a partir de la clave pública de la segunda entidad comunicante y;
- un segundo parámetro que indica la presencia o no de una firma de un conjunto de datos a firmar.

Según un modo de realización, la primera entidad comunicante comprende una memoria para almacenar una clave pública de una segunda entidad comunicante, comprendiendo el perfil de seguridad:

- un primer parámetro que indica la presencia o no de un cifrado de los datos útiles efectuado a partir de una clave simétrica y, llegado el caso, de la presencia de un cifrado de la clave simétrica a partir de la clave pública de la segunda entidad comunicante y;
- un segundo parámetro que indica la presencia o no de una firma de un conjunto de datos a firmar.

Según un modo de realización, el perfil de seguridad comprende:

- un tercer parámetro que indica la presencia o no de un cifrado efectuado a partir de la clave pública de la primera entidad comunicante bien de los datos útiles o bien de una clave simétrica y;
- un cuarto parámetro que indica la presencia o no de una firma de un conjunto de datos a firmar,

de por lo menos un mensaje que debe ser emitido por una segunda entidad comunicante como respuesta a un mensaje recibido de la primera entidad comunicante.

Según un modo de realización, el servidor comprende medios de acceso a la memoria que almacena los datos correspondientes a los identificadores de clientes y a los identificadores de equipos para revocar o suspender uno o varios equipo(s) o cliente(s).

Otro objetivo de la invención se refiere a un procedimiento, según uno de los modos de realización anteriores, que comprende, previamente, la ejecución de un procedimiento de generación de una petición de inscripción por una primera entidad comunicante con destino a una segunda entidad comunicante. El procedimiento de generación de una petición de inscripción comprende:

- Una activación del procedimiento de inscripción;
- Una generación de una petición de inscripción que consta de un identificador de un equipo, un identificador del usuario, una contraseña del usuario y una clave pública de la primera entidad comunicante;
- Un cifrado de la petición con una clave pública de la segunda entidad comunicante y una emisión de la petición de inscripción por medio de una interfaz de comunicación con destino a la segunda entidad comunicante.

Según un modo de realización, el procedimiento de generación de una petición de inscripción por una primera entidad comunicante comprende previamente:

- Una creación de una cuenta de usuario que comprende un identificador y una contraseña;
- El registro de los datos de dicha cuenta de usuario en una memoria de la segunda entidad comunicante;
- Una adquisición de una clave pública de la segunda entidad comunicante para la cual se emprende el procedimiento de inscripción desde la primera entidad comunicante;
- Una generación de un par de claves asimétricas de la primera entidad comunicante.

Según un modo de realización, el procedimiento de inscripción comprende las siguientes etapas realizadas por la segunda entidad comunicante:

- Una recepción de una petición de inscripción generada por un procedimiento de generación de una petición de inscripción de la invención;
- Un descifrado de los datos de la petición de inscripción por medio de una clave privada de la segunda entidad comunicante;
- Una comparación entre el identificador de usuario recibido y la contraseña de usuario recibida, con datos de cuentas de cliente almacenados en una memoria de la segunda entidad comunicante;
- Un registro del identificador del equipo en una memoria de la segunda entidad comunicante;
- Un registro de la clave pública de la primera entidad comunicante asociada al identificador del equipo en una memoria de la segunda entidad comunicante.

Según un modo de realización, la segunda entidad comunicante pone en práctica las siguientes etapas del procedimiento de inscripción:

- un control de una fecha actual con una fecha de referencia;
- una generación de un mensaje con destino a la primera entidad comunicante que comprende un código específico que indica que se debe renovar un par de claves asimétricas;
- una recepción de una nueva petición de inscripción generada por la primera entidad comunicante según el procedimiento de inscripción de la invención.

Otro objetivo de la invención se refiere a una entidad comunicante que comprende por lo menos una memoria, un módulo de cálculo y una interfaz de comunicación para la ejecución del procedimiento de comunicación de la invención y/o del procedimiento de inscripción.

Otro objetivo de la invención se refiere a un programa de ordenador que consta de un conjunto de instrucciones para la puesta en práctica del procedimiento de comunicación. En este modo de realización, un soporte físico, tal como una memoria, permite registrar las instrucciones y un módulo de cálculo permite poner en práctica las etapas del procedimiento. En este último caso, el programa de ordenador está configurado para ejecutar el procedimiento de la invención en un ordenador, una tableta, un *Smartphone* o, de manera más general, un equipo electrónico inteligente que comprende una interfaz de comunicación.

Según un modo de realización, el programa de ordenador está configurado para formar una API, que designa “Application Programming Interface”. Esta última se puede poner en práctica en un programa de ordenador en el seno de un procedimiento de gestión de una interfaz de comunicación de un equipo.

Según un modo de realización, un programa de ordenador está concebido también para comprender instrucciones y medios para la ejecución del procedimiento de inscripción. De manera idéntica, este programa de ordenador puede estar concebido para formar una API.

Breve descripción de las figuras

Se pondrán de manifiesto otras características y ventajas de la invención a partir de la lectura de la descripción detallada que se ofrece a continuación, en referencia a las figuras adjuntas, las cuales ilustran:

- figura 1: un esquema fundamental de los principales elementos del sistema de la invención que ponen en práctica los procedimientos de la invención;
- figuras 2A, 2B: las principales etapas de los procedimientos de la invención de generación de una petición de inscripción y de recepción de la petición de inscripción;
- la figura 3: las principales etapas del procedimiento de comunicación de la invención.

Descripción

La invención se refiere a la securización y la autentificación de comunicaciones entre dos entidades comunicantes. La descripción detalla un modo de realización en el cual las dos entidades se refieren, respectivamente, a un cliente y a un servidor. La presente invención tiene como finalidad un procedimiento de inscripción entre por lo menos dos entidades y un procedimiento de comunicación entre por lo menos estas dos entidades.

Cliente

Un cliente según la invención comprende como mínimo un módulo de cálculo, una memoria y una interfaz de comunicación. Según un modo de realización, el cliente es un ordenador, una tableta, un *smartphone* o incluso un equipo industrial de tipo caja inteligente o cualquier equipo electrónico dedicado para la aplicación que tiene como finalidad transferir datos de manera securizada. El cliente comprende un sistema operativo y un conjunto de funciones que permiten ofrecer a un usuario un conjunto de servicios en el seno de una red.

Por lo tanto, el cliente está asociado a un equipo. En la descripción que se ofrece a continuación, se hablará indiferentemente de un equipo o de un cliente, cuando el cliente es una entidad comunicante que tiene una configuración que le permite identificarse en el seno de una red. El cliente comprende, por tanto, un identificador indicado como EQ_ID. El equipo de cliente se indica, por tanto, indistintamente, como EQ_A, EQ_B o incluso CLIENTE de una manera general.

Consecuentemente, el cliente es, en general, una entidad que es capaz de iniciar una comunicación mediante un procedimiento de inscripción que tiene como objetivo securizar una transferencia de datos entre dicho cliente y un servidor.

Servidor

Un servidor según la invención comprende como mínimo una memoria y un módulo de cálculo así como una interfaz de comunicación. Según un modo de realización, el servidor es un ordenador conectado a una red, tal como la red internet. Según un modo de realización, el servidor está configurado para recibir mensajes provenientes de diferentes clientes y almacenar datos enviados por diferentes clientes. Según un modo de realización, el servidor almacena, en una base, de datos de una pluralidad de usuarios, entre ellos cuentas de cliente y asociaciones entre cada cliente y equipos de usuarios EQ. Además, el servidor almacena datos criptográficos.

El servidor es un equipo que pone a disposición una clave pública KSpub para uno o varios cliente(s). Esta clave pública permite cifrar mensajes emitidos por el cliente para el servidor.

El servidor de datos de la invención es un servidor que ofrece servicios a un cliente. Por tanto, el servidor de la invención no es un servidor de autentificación que realiza exclusivamente las funciones de autentificación en el sentido de un tercero de autentificación acoplado con otro servidor de datos. Uno de los objetivos de la invención es permitir el establecimiento de comunicaciones securizadas entre por lo menos un cliente y un servidor de datos ofreciendo servicios que implican una conexión securizada.

Cuenta de cliente

En la descripción que prosigue, un usuario se identifica con un Identificador USER_ID. El usuario es capaz de definir una cuenta y de referenciarla ante el servidor, por ejemplo, por medio de un enlace distante que permite registrar los datos de su cuenta. La cuenta comprende como mínimo un identificador USER_ID y una contraseña USER_MDP que está asociada al identificador USER_ID.

El procedimiento de intercambio de datos entre dos entidades comunicantes comprende, por tanto, previamente, una etapa de registro de un usuario en la entidad que define al servidor de datos.

Gestión de claves asimétricas

El método de autentificación de la invención se basa en una generación de un par de claves criptográficas asimétricas y el intercambio de claves públicas entre las entidades comunicantes. Un equipo genera una clave pública Kpub y una clave privada Kpriv, indicándose esta etapa con K_GEN en la figura 1. Esta función se puede realizar por medio de un componente criptográfico de *software* o de *hardware* del equipo. Entre las entidades comunicantes solamente se intercambian las claves públicas:

- la clave privada de cada cliente KApriv se almacena en una memoria de un equipo de cliente o en un componente de seguridad dedicado como, por ejemplo, un TMP que designa “Trusted Platform Module”, y;
- la clave privada de un servidor de datos KSpriv se almacena en una memoria del servidor.

Las claves privadas KApriv, KSpriv no se intercambian entre las entidades comunicantes durante la ejecución de los procedimientos de la invención.

En la figura 1, lado del cliente, las claves son gestionadas por un componente criptográfico indicado K_SUP_C. Este componente permite almacenar la clave privada KApriv y la clave pública KApub del cliente, así como la clave pública del servidor KSpub adquirida durante una etapa previa.

La figura 1 representa, además, un componente criptográfico del lado del servidor K_SUP_S que permite almacenar el par de claves asimétricas del servidor: KSpriv, KSpub.

En la presente invención, cada equipo está asociado a una clave privada única de un equipo KApriv que, eventualmente, puede renovarse. Una clave privada de un equipo KApriv está asociada a un equipo EQ_A como, por ejemplo, un *smartphone*, una tableta, un PC o un equipo industrial de tipo caja inteligente, tal como, por ejemplo, un contador eléctrico.

Un usuario está asociado a uno o varios equipos EQ_A, EQ_B, etcétera.

Procedimiento de generación de una petición de inscripción

La inscripción es una etapa preliminar a cualquier transmisión de datos útiles entre dos entidades comunicantes que establecen una comunicación securizada según el procedimiento de comunicación de la invención. La inscripción permite intercambiar datos entre las entidades comunicantes que permitirán la securización de los intercambios de datos.

Cuando un cliente procede a una inscripción ante un servidor, el mismo inicia este procedimiento generando una petición REQ_E. Una de las ventajas es que esta petición no comprende la emisión de una clave privada del equipo. El cliente comprende un componente indicado como ENROL_C que permite poner en práctica el mecanismo de inscripción desde el punto de vista del servidor, en especial para generar las peticiones de inscripción REQ_E.

Desde el punto de vista del servidor, un componente indicado como EQ_MG controla la gestión de los equipos y de los usuarios y procesa las peticiones de inscripción REQ_E, en particular verificando la validez de los datos de la petición. Cuando un equipo es inscrito por un servidor, su identificador se almacena en una memoria del servidor. El servidor es, entonces, capaz de asociar un cliente con un conjunto de equipos asociados que han sido inscritos por el usuario. En el lado del servidor, la función que gestiona los equipos y los usuarios se indica como MG en la figura 1 y la función que procesa las peticiones de inscripción se indica como ENROL_S. Una memoria permite almacenar las claves públicas de los equipos así como las contraseñas de las cuentas de cliente. Esta memoria se indica como K_PUB en la figura 1.

El procedimiento de inscripción de la invención se fundamenta en la creación de una cuenta del cliente por un usuario cuyos datos se almacenan en una memoria de un servidor de datos, definiendo el servidor de datos SERV una de las entidades comunicantes de la invención.

La figura 2A representa las etapas principales de un procedimiento de generación de una petición de inscripción REC_E emprendida por el procedimiento de generación de una petición de inscripción M1_ENROL_C realizado por un equipo tal como un cliente.

Antes de comunicarse con un servidor según el procedimiento de comunicación de la invención, cada cliente materializa una fase de inscripción según el procedimiento de generación de una petición de inscripción de la invención.

El procedimiento M1_ENROL_C comprende una etapa que activa este procedimiento que se corresponde asimismo con la etapa epónima del método M1_ENROL_C.

El procedimiento de generación de una petición de inscripción M1_ENROL_C por el cliente comprende una etapa que se corresponde con la adquisición de una clave pública de un servidor SERV, indicada como ACQ_KSpub. Según los modos de realización de la invención, la etapa de adquisición de la clave pública del servidor KSpub se puede considerar como formando parte del procedimiento de inscripción o la misma puede considerarse como una etapa previa en la cual la clave pública del servidor KSpub ha sido adquirida por un usuario antes de que el mismo emprende la inscripción. En este último caso, la adquisición de la clave pública del servidor KSpub no está comprendida en el procedimiento de inscripción.

Esta etapa se puede realizar mediante una entrada manual si un usuario copia una clave pública de un servidor KSpub en una interfaz de un equipo de cliente. Además, la clave pública del servidor KSpub se puede recibir de un equipo tercero o incluso directamente del servidor SERV que forma una de las dos entidades comunicantes de la invención. En este último caso, la clave pública del servidor KSpub se puede recibir, por ejemplo, después de la creación de una cuenta de usuario ante el servidor SERV. Según otros ejemplos de realización, la adquisición de la clave pública del servidor KSpub se puede generar por medio de un archivo tal como una imagen, un código *captcha*, un código de barras o un código 2D, tal como un código QR. La adquisición de la clave pública del servidor KSpub por parte del cliente se puede realizar, en este último caso, mediante una lectura del código o de la imagen que comprende dicha clave por medio del equipo. El equipo comprende, en este último caso, medios de captura de una imagen tal como un sensor óptico.

Según un modo de realización, cuando ya ha tenido lugar la adquisición de la clave pública KSpub del servidor, la clave pública del servidor se considera como ya almacenada en una memoria del equipo. La etapa de adquisición de la clave pública del servidor KSpub del procedimiento se puede corresponder, por tanto, con la adquisición de esta clave desde la memoria del equipo cuando la misma ya ha sido adquirida del servidor. Cuando el equipo no tiene la clave pública del servidor, la adquisición comprende la operación que tiene como objetivo recuperar esta clave pública KSpub del servidor. Esta operación puede ser el resultado de una operación que tiene como objetivo

establecer un diálogo entre el cliente y el servidor. Según otro modo de realización, el usuario recupera la clave pública del servidor sin proceder a un intercambio entre el cliente y el servidor, por ejemplo mediante una copia manual de la clave en una interfaz del cliente.

Cada equipo que procede a una inscripción con un servidor ha almacenado una clave pública KSpub de dicho servidor. La clave pública del servidor KSpub permite cifrar la petición de inscripción así como los mensajes emitidos durante el procedimiento de comunicación de la invención.

Según un modo de realización de la invención, el procedimiento de generación de una petición de inscripción por parte del cliente comprende una etapa de generación de una clave pública de un equipo EQ_A, indicada como KApub, y de una clave privada de un equipo indicada como KApriv. Las etapas de generación se indican, respectivamente, como GEN_KApub y GEN_KApriv en la figura 2A, y, además, se generan generalmente al mismo tiempo. En este último caso, se genera conjuntamente un par de claves. Cuando la etapa de generación del par de claves asimétricos se ha efectuado de manera previa, el procedimiento de generación de una petición de inscripción tiene como objetivo extraer la clave pública del equipo KApub de una memoria del equipo para incluirla en la petición. En este último caso, según un modo de realización, el procedimiento de generación de una petición de inscripción comprende únicamente la adquisición en una memoria del equipo, de la clave pública del cliente y no su generación en cada inscripción.

El procedimiento de generación de una petición de inscripción REQ_E por parte del cliente comprende, por tanto, la generación de una petición de inscripción REQ_E con destino al servidor SERV. Esta etapa se indica como GEN_REQ en la figura 2A. Esta etapa es realizada por un módulo de cálculo del cliente indicado en la figura 1 como: “REQ”. La misma comprende la recuperación de un cierto número de datos almacenado en una memoria del cliente y la generación de la petición REQ_E que comprende estos datos recuperados. Las etapas de recuperación de ciertos datos son realizadas asimismo durante el procedimiento de comunicación de la invención. En especial, el identificador del equipo y el identificador de usuario se utilizan en cada transmisión de mensajes nuevos mediante aplicación del procedimiento de comunicación de la invención. Ciertas etapas que prosiguen son, por tanto, comunes al procedimiento de inscripción y el procedimiento de comunicación de la invención.

Según un modo de realización, el módulo de cálculo recupera datos de por lo menos una memoria del cliente, por ejemplo almacenada en una base de datos, entre ellos un identificador del equipo indicado como EQ_ID. Además, el módulo de cálculo recupera el identificador de usuario USER_ID. El identificador de usuario USER_ID puede:

- o bien recuperar por parte del módulo de cálculo desde una memoria en la cual un usuario ha almacenado previamente su identificador;
- o bien recuperar desde un control de entrada de una interfaz de usuario en la cual el usuario indica su identificador sin que el mismo se almacene previamente en el equipo.

El módulo de cálculo recupera asimismo una contraseña de usuario USER_MDP. La contraseña de usuario USER_MDP se puede recuperar, asimismo, o bien de una memoria del equipo EQ_A en la cual la misma ha sido almacenada previamente por un usuario del equipo EQ_A, o bien de un control de entrada de una interfaz de usuario. Esta etapa es ejecutada en especial por el procedimiento de inscripción.

Además, el módulo de cálculo recupera la clave pública del equipo KApub del equipo EQ_A que está almacenada en una memoria del equipo EQ_A después de su generación o su recuperación desde una interfaz. La clave pública del cliente se transmite durante el procedimiento de inscripción, pero no necesariamente durante el procedimiento de comunicación de la invención. Es precisamente una ventaja de la invención el no retransmitir la clave pública del equipo en cada emisión de mensajes nuevos.

La petición de inscripción así generada comprende, por tanto, los siguientes datos:

- el identificador de usuario, USER_ID;
- la contraseña del cliente, USER_MDP;
- el identificador del equipo, EQ_ID;
- la clave pública del cliente, KApub.

El procedimiento de generación de una petición de inscripción comprende una etapa de cifrado de la petición, indicada como CRYP_REQ en la figura 2A, mediante la clave pública del servidor KSpub. Esta clave pública ha sido adquirida previamente por el cliente y se puede utilizar para cifrar la petición de inscripción. Consecuentemente, el servidor estará en condiciones de descifrar la petición así cifrada gracias a su clave privada KSpriv.

Según una alternativa de realización, la clave pública del servidor KSpub se utiliza para cifrar una clave simétrica. Esta solución es más eficaz en términos de cálculo que un algoritmo de cifrado del mensaje efectuado a partir de claves asimétricas. Esta solución permite cifrar un mensaje más corto con una clave asimétrica que comprende la

clave asimétrica. En la recepción, la clave privada KSpriv del servidor permite descifrar la clave simétrica y descodificar el mensaje cifrado con la clave simétrica así descifrada. Esta alternativa se puede poner en práctica durante el procedimiento de inscripción y/o durante el procedimiento de comunicación de la invención.

El procedimiento de inscripción se efectúa previamente a la emisión de mensajes según el procedimiento de comunicación de la invención.

La inscripción se puede efectuar de una vez por todas desde el equipo de cliente o desde cualquier equipo que permita establecer un enlace con el servidor de datos.

Según otro ejemplo de realización, la inscripción puede ser una etapa preliminar a la emisión de un mensaje, que sucede directamente a la etapa de transmisión securizada de mensajes.

Recepción de la petición por el servidor

La invención se refiere al procesado M2_ENROL_S de una petición de inscripción REQ_E recibida por el servidor. Cuando el servidor recibe una petición de inscripción REQ_E nueva, el mismo procede a su recepción REC_REQ por medio de una interfaz de comunicación, como, por ejemplo, una tarjeta de red. El servidor emprende una etapa de descifrado de los datos, indicada como DECRYPT_REQ, por medio de su clave privada KSpriv.

A continuación, los datos descifrados se extraen y se almacenan en una memoria del servidor. El servidor efectúa un control del identificador de usuario USER_ID y de la contraseña del usuario MDP_USER los cuales son datos ya registrados en una memoria del servidor durante la creación de la cuenta de cliente en el servidor SERV.

Cuando los datos de la cuenta de usuario recibidos se corresponden con los datos ya registrados, el servidor registra los datos del equipo, entre ellos su identificador EQ_ID y la clave pública del equipo KApub, en una memoria.

El servidor SERV procede entonces a una asociación ASSO_KApub entre los datos de los equipos y una cuenta de usuario. Así, un usuario se puede asociar a diferentes equipos cuyas claves públicas son conocidas por el servidor.

Renovación de clave

Según un modo de realización, un mecanismo de renovación de claves emprende la renovación de un par de claves asimétricas: se renuevan una clave privada del equipo KApriv y una clave pública del equipo KApriv.

La clave pública del equipo KApub se puede transmitir de nuevo con destino al servidor. Para ello, se puede reiterar un procedimiento de inscripción, por ejemplo bajo demanda del servidor o después de que haya transcurrido un cierto tiempo. Según un ejemplo de puesta en práctica, el servidor puede emitir un mensaje de error tras la recepción de un mensaje de cliente cuya clave pública ya no es válida. El mensaje de error puede comprender un código de rechazo que indica que debe reconducirse un procedimiento de inscripción con una clave pública nueva.

De forma idéntica, cuando es la clave pública del servidor la que se modifica, un mensaje de error puede indicar al cliente que es necesario que el mismo recupere una nueva clave pública del servidor.

Este mecanismo se puede emprender de forma automática y de manera transparente con respecto a un usuario. El equipo renueva, entonces, una clave privada nueva KApub que se almacena localmente y renueva una clave pública nueva KApub asociada a esta clave privada. La clave pública del equipo es enviada, entonces, mediante una nueva petición de inscripción al servidor.

Transmisión de los datos útiles

El procedimiento de comunicación de la invención permite emitir y recibir datos en forma de mensajes entre dos entidades comunicantes, indicándose estos mensajes con MES_C y MES_S en la figura 1. El procedimiento de la invención permite intercambiar comunicaciones de manera securizada por la definición de mensajes cuya seguridad es “autoportante”, es decir, que cada mensaje intercambiado comprende sus propias informaciones de seguridad que permiten procesar y cifrar el mensaje enviado. La invención no necesita que un establecimiento de una sesión entre las dos entidades comunicantes garantice un canal securizado entre dichas dos entidades. La invención comprende, por tanto, dos mecanismos que permiten definir un método de comunicación securizado entre dos entidades comunicantes:

- un mecanismo de inscripción y;
- un mecanismo de generación de encabezamiento de autentificación de los mensajes de datos transmitidos entre las dos entidades.

La invención se refiere a cada uno de estos dos mecanismos.

La descripción que prosigue describe un modo de realización en el cual el cliente emite un mensaje hacia el

servidor, siendo verificado este mensaje por el servidor. La invención se refiere, asimismo, a los intercambios contrarios de mensajes, entre ellos particularmente un mensaje cuyo encabezamiento es generado por el servidor y cuya verificación es efectuada en la recepción por parte de un cliente. Según un modo de realización, el procedimiento de comunicaciones securizadas de la invención es simétrico entre un cliente y un servidor. El procedimiento de comunicación se aplica, por tanto, recíprocamente, de una transmisión de un cliente hacia un servidor o de un servidor hacia un cliente.

En la figura 1 se indican los componentes que permiten procesar las funciones de emisión y de recepción de los procedimientos de la invención: SEC_SW_C para el cliente y SEC_SW_S en el lado del servidor.

Encabezamiento de autentificación de un mensaje

A continuación de la etapa de inscripción, la invención pone en práctica un procedimiento de comunicación que permite transmitir mensajes securizados mediante la generación de un encabezamiento de autentificación, indicado como TOKEN. El procedimiento de comunicación, en otra variante de realización, se podría realizar de forma independiente con respecto a la ejecución previa de un procedimiento de inscripción. Esto es así, por ejemplo, cuando los datos intercambiados en el procedimiento de inscripción fuesen definidos por un usuario en cada equipo, como por ejemplo el intercambio de las claves públicas y de los identificadores de equipo y de usuario.

El encabezamiento de autentificación TOKEN es generado por un componente del cliente indicado en la figura 1 como: TOK_GEN_C. En el lado del servidor, el componente indicado como TOK_CHK_S verifica el encabezamiento de autentificación recibido del cliente. A la inversa, cuando un mensaje es emitido por el servidor con destino a un cliente, un componente indicado como TOK_GEN_S, en el lado del servidor, permite generar el encabezamiento de autentificación del mensaje y un componente indicado como TOK_CHK_C, en el lado del cliente, permite verificar el encabezamiento de autentificación de un mensaje emitido por el servidor con destino al cliente.

El encabezamiento de autentificación TOKEN de los mensajes transmitidos comprende diferentes campos de datos, entre ellos el identificador del equipo EQ_ID, el identificador del usuario USER_ID, la identificación del mensaje, MES_ID, un perfil de seguridad PRO_SEC y una firma llegado el caso.

El encabezamiento de autentificación TOKEN se puede integrar, por ejemplo, en los encabezamientos del protocolo de transporte utilizado según las comunicaciones efectuadas, como un encabezamiento del protocolo HTTP por ejemplo.

Según un modo de realización, el encabezamiento de autentificación se añade a la lista de los encabezamientos del protocolo aplicativo de transporte utilizado por la aplicación. En el ejemplo del protocolo HTTP, según un modo de realización, el contenido del encabezamiento de autentificación generado por la presente invención se asocia al encabezamiento “Authorization:” del protocolo HTTP/1.1 según la RFC [2616].

Identificador de mensaje, MES_ID

Según un modo de realización, el módulo de cálculo recupera un identificador de mensaje MES_ID que es generado por un contador de mensajes el cual genera identificadores de mensajes. La figura 1 representa los componentes que permiten generar y procesar identificadores de mensajes, indicándose también los mismos como MES_ID.

Según un modo de realización, el contador de mensajes calcula el MES_ID a partir de un factor aleatorio, es decir de un parámetro aleatorio y de una fecha. El factor aleatorio permite definir un identificador único del mensaje.

Cuando el identificador del mensaje MES_ID se calcula en particular a partir de una fecha definida por un reloj local del equipo, el identificador MES_ID comprende una información relativa a la fecha de generación del mensaje que se podría descodificar en la recepción por parte del servidor.

Según una alternativa de realización, el MES_ID se puede generar con un parámetro no aleatorio y una fecha.

El identificador de mensaje MES_IS se puede calcular, por ejemplo, sobre la marcha, es decir en tiempo real por parte de un módulo de cálculo de la entidad comunicante. El identificador del mensaje así calculado se asigna a un mensaje.

Perfil de seguridad

El perfil de seguridad PRO_SEC permite definir un algoritmo que se utilizará para afirmar o cifrar el contenido a transmitir y para indicar y definir si la respuesta emitida por el servidor se debe cifrar también y según qué algoritmo.

Las diferentes entidades comunicantes, tales como un servidor y una pluralidad de clientes, pueden comprender una configuración de perfiles de seguridad predefinidos. Cada perfil predefinido se puede activar para definir una manera de emitir y recibir datos con otra entidad.

Según un modo de realización de la invención, se predefinen cuatro perfiles de seguridad.

Un primer perfil se corresponde con la activación de un parámetro de seguridad P1 incorporado en el encabezamiento de autentificación TOKEN del mensaje a transmitir por el cliente al servidor. Este parámetro indica la presencia de un cifrado de los datos útiles transmitidos. Así, el servidor que recibe este parámetro es capaz de poner en práctica un descifrado de los datos transmitidos cuando estos últimos están cifrados.

Un segundo perfil se corresponde con la activación de un parámetro de seguridad P2 incorporado en el encabezamiento de autentificación del mensaje a transmitir por el cliente. El parámetro P2 permite indicar que el encabezamiento de autentificación está firmado. La firma es efectuada, en este caso, por el cliente gracias a la clave privada del cliente KApriv. Según un modo de realización, la firma se incorpora en el encabezamiento de autentificación.

Un tercer perfil se corresponde con la activación de un parámetro de seguridad P3 incorporado en el encabezamiento de autentificación TOKEN del mensaje a transmitir por el cliente al servidor. Este parámetro indica que los datos útiles del o de los mensaje(s) de retorno emitidos por el servidor hacia el cliente deben estar cifrados.

Un cuarto perfil se corresponde con la activación de un parámetro de seguridad P4 incorporado en el encabezamiento de autentificación TOKEN del mensaje a transmitir por el cliente. El parámetro P4 indica al servidor que el mismo debe firmar los encabezamientos de autentificación de los mensajes que emitirá como retorno del mensaje emitido por el cliente.

Así, si los parámetros P3 y P4 son activados por el cliente en los mensajes emitidos hacia el servidor, el servidor cifrará los datos útiles y firmará el encabezamiento de autentificación TOKEN de los mensajes emitidos a su vez hacia el cliente como respuesta al(a los) mensaje(s) recibido(s) de este último.

El servidor puede, por tanto, indicar, a su vez, el valor de los parámetros P1, P2, P3 y P4 para informar al cliente sobre su modo de cifrado de los datos así como la presencia de una firma.

Esta configuración tiene la ventaja de permitir el establecimiento de comunicaciones cuya seguridad es totalmente autoportante entre dos entidades comunicantes.

Cuando el procedimiento se implementa de forma simétrica en el cliente y el servidor, el encabezamiento de autentificación de la respuesta del servidor comprende, por tanto, también, un perfil de seguridad que comprende una parametrización P1, P2, P3, P4. En este caso, la firma se genera a partir de la clave privada del servidor KSpriv y el cifrado de los datos útiles se efectúa con la clave pública del cliente KApub.

Los diferentes perfiles de seguridad permiten adaptar el nivel de seguridad de los intercambios de datos entre las entidades comunicantes según el contexto de intercambios de datos o del tipo de datos a intercambiar.

Según un modo particular de realización de la invención, los perfiles de seguridad PRO_SEC utilizan un quinto parámetro de seguridad P5 representativo del formato de la firma utilizada para el encabezamiento de autentificación. Este parámetro permite definir la utilización o no en la firma de:

- uno o varios campos de datos del encabezamiento de autentificación TOKEN del mensaje;
- datos útiles y;
- de datos del protocolo de transporte tales como los encabezamientos del protocolo de transporte, o de otros campos de datos tales como el campo de tipo REQUEST_LINE del protocolo http.

Según otro modo de realización, los parámetros de seguridad P2 y P4 indican directamente el formato de firma aplicado.

El formato de una firma se define mediante al menos uno cualquiera de estos datos o una combinación de estos datos:

- El algoritmo de la función *hash*;
- El algoritmo de cifrado;
- El tipo de clave;
- La indicación de los datos a firmar tal como, por ejemplo, los campos de datos del encabezamiento de autentificación así como los datos útiles y, opcionalmente, datos relativos a los campos de datos del protocolo de transporte utilizado.

Cuando una entidad recibe un perfil de seguridad que la misma no conoce, es decir, que no está predefinido en una memoria de la entidad, entonces se puede utilizar un perfil por defecto. Según otro modo de realización, la etapa de inscripción puede comprender la transmisión de la definición de un perfil de seguridad o bien en el encabezamiento de autentificación TOKEN de datos, o bien en la carga útil de los datos transmitidos. En la recepción, una entidad

puede registrar, entonces, la definición del perfil nuevo de seguridad y utilizarlo para desplegar una estrategia de cifrado de los mensajes emitidos y de descifrado de los mensajes recibidos.

Además, el perfil de cifrado comprende la designación de un algoritmo de generación de firma como, por ejemplo, RSA-SHA256, y, llegado el caso, la designación de un algoritmo de cifrado de los datos, como, por ejemplo, el AES.

El perfil de seguridad comprende, por tanto, una indicación sobre la presencia de una firma y sobre la presencia de un cifrado de los datos y, llegado el caso, el perfil de seguridad comprende la designación de los algoritmos utilizados para generar la firma o cifrar los datos.

Firma

El encabezamiento de autentificación TOKEN comprende, asimismo, una firma de los datos transmitidos en el encabezamiento y/o en el cuerpo de mensaje. Una firma se crea por medio de un algoritmo de generación de una firma. La firma se realiza por medio de una clave privada de la entidad comunicante que firma. Si el cliente firma el encabezamiento de autentificación de un mensaje emitido, la firma se realiza a partir de la clave KApriv, es decir, la clave privada del equipo. Según un modo de realización, la invención puede poner en práctica un algoritmo basado en un método RSA SHA256 para generar la firma. Cabe recordar que el acrónimo SHA designa, en la terminología anglosajona: “Secure Hash Algorithm” y se corresponde con una función *hash* criptográfica. El RSA es un algoritmo de criptografía simétrica que utiliza un par de claves asimétricas. Los dos algoritmos pueden estar asociados en un único algoritmo de cifrado.

Según otro ejemplo de realización, puede utilizarse, según el método de la invención, el algoritmo ECDSA que designa “Elliptic Curve Digital Signature Algorithm”. Se trata de un algoritmo de firma digital con clave pública.

El algoritmo de generación de una firma se puede determinar automáticamente en función del equipo del cliente o de su sistema operativo. Una ventaja consiste en utilizar los recursos ya existentes en un equipo.

Según un modo de realización, cuando un campo del encabezamiento de autentificación TOKEN comprende la firma generada, en el encabezamiento se puede completar otro campo para designar el algoritmo que permite generar la firma y/o el algoritmo de cifrado de los datos útiles. En la recepción, el servidor de datos podrá descodificar la firma gracias a la elección del algoritmo correcto para descodificar la firma.

La firma se genera a partir de datos relativos, en especial, al cliente y al equipo.

Según un ejemplo de realización, la firma se genera a partir de los datos: MES_ID, EQ_ID, USER_ID, PRO_SEC y del contenido del mensaje.

Según otro modo de realización, la firma se genera a partir de los datos útiles del mensaje. Esto permite generar una firma de los datos de autentificación MES_ID, EQ_ID, USER_ID, del perfil de seguridad PRO_SEC, y del contenido del mensaje DATA. Los datos, cuando están firmados, se pueden corresponder con los datos útiles cifrados o con los datos útiles no cifrados.

Según un modo de realización, la firma puede tener en cuenta datos de un mensaje del protocolo de transporte que encamina los mensajes intercambiados tales como datos de encabezamiento de protocolo, de la dirección del mensaje del protocolo o incluso de otro campo propio del protocolo como, por ejemplo, la línea de petición del protocolo http.

El término “encabezamiento de protocolo” se utiliza para diferenciarlo del encabezamiento de autentificación de la invención.

A título de ejemplo, los diferentes campos del protocolo http del siguiente ejemplo se pueden utilizar según un modo de realización de la invención para firmar el encabezamiento de autentificación. La petición http presenta, por ejemplo, la siguiente forma:

- Encabezamiento:

POST http://control_center_url/rest/conso HTTP/1.0

Accept: application/json

User-Agent: Mozilla/4.0 (compatible; MSIE 5.0 ; Windows 95)

Authorization: JohnDo:Android22434:1430896533037_97:OneWaySignature_RSA-SHA256_none: w9Bgirb8.....

- Cuerpo de mensaje (*body*):

{“PI”=2345, “HCHC”=29384632, “HCHP”=2936241490}

Según un modo de realización, pueden utilizarse uno o varios datos relativos a los datos del protocolo de transporte. También puede utilizarse una parte de un campo de un encabezamiento del protocolo. Según un ejemplo, el campo *Method* del protocolo http que precisa el tipo de petición, entre ellos en especial los valores {GET, PUT, POST}, presente en la línea de petición de una petición http, resulta interesante para firmar el encabezamiento de autentificación TOKEN. Esta consideración permite en especial evitar los ataques de tipo “repetición” por parte de un tercero realizando otra acción diferente a la petición inicial.

Según un ejemplo de realización, un encabezamiento de mensaje de un protocolo aplicativo de transporte se define por medio de un par {clave :valor}. Por ejemplo, para el protocolo HTTP, el encabezamiento [Caducidad: “Sat, 07 Nov 2015 00:59:59 GMT”] representa una fecha de caducidad de la petición. Según este mismo protocolo, el tipo de petición y la dirección del recurso a consultar están contenidos en la línea de petición del mensaje, por ejemplo [POST http://control_center_uri/rest/conso HTTP/1.1], y se pueden utilizar para generar la firma.

Este modo de realización es particularmente ventajoso para garantizar la integridad de los intercambios de datos.

Según este mismo ejemplo, cuando los datos se firman con el par [Caducidad: “Sat, 07 Nov 2015 00:59:59 GMT”], y con el tipo de la petición HTTP, que, en este caso, es una petición de tipo “POST”, no es posible que un tercero emprenda un ataque por repetición reutilizando los mismos datos con un tipo de petición diferente o/y con una fecha de expiración diferente, ya que, en este caso, la firma no será reconocida por el servidor.

La generación de una firma comprende la ejecución de una función *hash* de los datos a firmar. Así, si un tercero, no autorizado, recupera un mensaje firmado, no es posible reconstruir los datos que se han firmado a partir de la firma. La consideración del identificador del mensaje MES_ID, que cambia en cada mensaje, en la firma permite, gracias a la función *hash*, generar un contenido de la firma totalmente diferente de un mensaje a otro.

La generación de una firma puede comprender, asimismo, una función de *padding*, es decir una función de llenado de los datos.

Finalmente, la firma se genera a partir de la clave privada del cliente KApriv.

Las entidades comunicantes de la invención comprenden medios para generar un par de claves asimétricas KApriv, KApub, de manera que la clave privada KApriv permite generar una firma de un encabezamiento de autentificación de un mensaje emitido por una entidad comunicante mediante la ejecución de una función *hash* y de una función de llenado de los datos.

Cifrado de los datos

Cuando la opción del cifrado de los datos de un mensaje emitido por el cliente está activada, el perfil de cifrado define qué algoritmo se utiliza para cifrar los datos. El perfil de cifrado se indica en el encabezamiento de autentificación TOKEN del mensaje y permite indicar la designación del algoritmo de cifrado. Esta designación se puede codificar en el mismo campo que la designación del algoritmo de la generación de una firma. Los datos del mensaje que se transmiten al servidor se cifran con el algoritmo determinado por el cliente. Los datos a continuación se pueden descifrar, en el lado del servidor, gracias a la indicación del algoritmo utilizado.

El algoritmo de cifrado de los datos se puede determinar de forma automática en función del equipo del cliente o de su sistema operativo. Una de las ventajas es la de utilizar los recursos ya existentes en un equipo.

Un ejemplo de algoritmo según la invención puede ser el AES que designa “Advanced Encryption Standard” en la terminología anglosajona. Se trata de una normativa de cifrado avanzada conocida también con la denominación de Rijndael. Según el procedimiento de la invención pueden utilizarse, alternativamente, otros algoritmos tales como Script o Vscript.

Según un modo de realización, los datos útiles se cifran a partir de la clave pública del servidor KSpub, es decir con la clave pública de una segunda entidad comunicante KSpub en el caso general en el que el servidor es una segunda entidad comunicante.

Según otro modo de realización, los datos se cifran gracias a una clave simétrica y la clave simétrica se cifra ella misma con una clave asimétrica, tal como la clave pública del servidor KSpub. Este modo de realización presenta la ventaja de optimizar las operaciones de cifrado sobre volúmenes de datos más pequeños, en especial relativos al tamaño de una clave simétrica en lugar de un tamaño de campo relativo a un contenido de datos.

Los perfiles de seguridad se pueden trasladar, entonces, a este caso concreto en el cual se precisa si un mensaje consta de un encabezamiento firmado y un contenido cifrado en un sentido y en el sentido de retorno. Un “contenido cifrado” significa, por lo tanto, en este caso, que el mismo se ha cifrado con una clave simétrica y que la clave simétrica se ha cifrado con una clave asimétrica.

Ventajas de la transmisión de campos en el encabezamiento

El campo MES_ID permite definir una seguridad contra los ataques por repetición de mensajes de terceros.

El campo EQ_ID permite definir una seguridad cuando un equipo ha sido suspendido o revocado por el servidor SERV.

El campo USER_ID permite definir una seguridad cuando una cuenta de usuario ha sido suspendida o revocada por el servidor SERV.

Según un modo de realización de la invención, cuando el servidor ha emprendido un procedimiento de suspensión o de revocación de un usuario, se suspende o revoca también el conjunto de los equipos asociado a este usuario.

La figura 3 representa las principales etapas del procedimiento de comunicación de la invención desde el punto de vista de una entidad comunicante que genera un mensaje MES.

La etapa de generación del TOKEN se indica como GEN_TOKEN. La misma comprende las subetapas de generación de un identificador de mensaje GEN_MES_ID y de inserción INSERT_MES_ID de este identificador en el encabezamiento de autentificación TOKEN.

La generación del TOKEN comprende, además, la inserción de un identificador de equipo INSERT_ED_ID y la inserción de un identificador de usuario INSERT_USER_ID.

Estas etapas permiten generar un encabezamiento de autentificación según el procedimiento de comunicación de la invención.

Cuando el TOKEN se firma SIGN_TOKEN, el mismo se puede firmar a partir de la clave privada del cliente KApriv.

Cuando se efectúa un cifrado CRYP_DATA, el mismo se puede realizar a partir de la clave pública KSpub del servidor.

El mensaje que consta del encabezamiento de autentificación y los datos útiles se puede generar, entonces, GEN_MES, según el protocolo utilizado para emitir datos entre el cliente y el servidor, como, por ejemplo, un protocolo HTTP.

Según una variante de realización, tal como se representa con línea de puntos en la figura 3, puede utilizarse una clave simétrica Ksym para cifrar los datos utilizados durante la ejecución de la etapa CRYP_DATA. En este modo de realización, la propia clave simétrica se puede cifrar a partir de la clave pública del servidor KSpub y se puede insertar, por ejemplo, en el encabezamiento de autentificación TOKEN durante la etapa INSERT_Ksym.

Servidor, Gestión de las inscripciones

El servidor de datos que se corresponde con una de las entidades comunicantes de la invención está destinado a gestionar transmisiones de datos con una pluralidad de clientes. A este efecto, comprende un componente que permite gestionar los equipos, indicándose el mismo con EQ_MG en la figura 1. Este componente permite almacenar los datos de cifrado de los equipos del cliente en una memoria indicada con K_PUB que almacena las claves públicas de los equipos KApub. Este componente comprende una función MG que está configurada para almacenar las cuentas de clientes y una función ENROL_S que permite recibir y procesar una petición de inscripción de un equipo. El procesado de una petición comprende operaciones de descifrado de los datos y operaciones de verificaciones que tienen como objetivo verificar que el equipo, el usuario o el mensaje recibidos no están suspendidos o revocados o que las cuentas del cliente ya existen correctamente.

Además, la función MG permite revocar o suspender equipos o usuarios. Esta acción se puede emprender automáticamente bajo demanda de un cliente o bajo demanda de un administrador del servidor.

Servidor – recepción de un mensaje, descifrado

El mensaje emitido por el equipo es recibido por el servidor por medio de una interfaz de comunicación. Un componente del servidor realiza una etapa de verificación del mensaje recibido.

El servidor comprende un juego de claves asimétrico que comprende una clave pública KSpub y una clave privada KSpriv. El mensaje recibido por el servidor se ha cifrado con la clave pública del servidor KSpub por parte del cliente. Esta clave pública del servidor KSpub ha sido adquirida previamente por un usuario, por ejemplo, por medio del equipo EQ_A.

Servidor – verificación del identificador de mensaje

La verificación del mensaje comprende el control del identificador del mensaje: MES_ID. El control de los datos MES_ID comprende la verificación de la fecha de generación del mensaje con una hora local del servidor. La fecha

de generación del mensaje se puede calcular a partir del identificador de mensaje MES_ID por medio de un módulo de cálculo y un algoritmo de descodificación adecuado. Cuando la desviación entre la fecha descodificada en el MES_ID y la fecha local del servidor supera un umbral predefinido, el servidor puede emprender una denegación del mensaje recibido. Cuando la desviación de fecha es inferior a un umbral de fecha predefinido, el servidor puede procesar el mensaje en la recepción.

Según un modo de realización, en caso de una desviación de fecha demasiado significativa, el servidor reenvía un error específico que contiene la fecha en curso del servidor. Esta variante permite que el cliente se pueda resincronizar y puede retransmitir un nuevo TOKEN válido.

La verificación del MES_ID por el servidor permite limitar los ataques de red por repetición de mensaje sobre un periodo más largo que el periodo de tiempo durante el cual es válido un mensaje a continuación del análisis del valor de los datos del MES_ID.

Una segunda verificación efectuada por el servidor consiste en verificar si el mensaje ya ha sido recibido por este último. Si el mensaje ya ha sido recibido, es decir que el MES_ID del mensaje recibido es idéntico a un MES_ID de un mensaje recibido anteriormente, entonces el mensaje no es procesado por el servidor.

Servidor – verificación de la autentificación, de la clave pública del cliente KApub

Cuando el MES_ID de un mensaje recibido por el servidor no es rechazado, entonces el servidor procede a una etapa de verificación de la autentificación del mensaje. Según los modos de realización, el servidor puede verificar alternativamente los datos de autentificación antes que el identificador MES_ID.

Cabe recordar que el usuario ha definido previamente una cuenta de usuario que comprende un identificador de usuario y una contraseña asociada. El servidor SERV ha almacenado los datos de esta cuenta de usuario en una memoria.

El servidor ejecuta una búsqueda de la clave pública del equipo KApub en su base de datos. La clave pública del equipo KApub se ha asociado al cliente cuya referencia USER_ID es conocida ya que la misma se ha almacenado como consecuencia del registro de la cuenta de cliente.

La clave pública del equipo KApub que está contenido en el mensaje transmitido se compara entonces con la clave pública del equipo almacenado en la memoria del servidor.

Cuando se produce una correspondencia de las claves públicas del equipo entre, por un lado, la transmitida en el mensaje, y, por otro lado, la almacenada en el servidor, puede efectuarse una validación del mensaje recibido. Según un modo de realización, la clave pública del equipo almacenada en el servidor se puede utilizar para verificar que la firma está autentificada correctamente, con lo cual el mensaje puede ser procesado por el servidor.

Si la clave pública del cliente KApub ha sido revocada o suspendida o incluso si la misma no es conocida por el servidor, entonces el mensaje no es procesado por este último. Según un modo de realización, cuando la firma es no válida, el mensaje es rechazado por el servidor.

Una ventaja de esta solución es que el servidor no almacena más que informaciones públicas de los clientes, es decir las claves públicas de los clientes KApub. Las claves privadas de los clientes no son almacenadas por el servidor. Como consecuencia, un tercero que acceda a la base de datos del servidor no puede recuperar las claves privadas de los clientes sin la autorización de estos últimos.

Verificación de la firma

Cuando los mensajes transmitidos están firmados, la clave pública del equipo KApub conocida por el servidor SERV se puede utilizar también para verificar la firma comprendida en el mensaje y que se ha realizado a partir de la clave privada del cliente KApriv. La firma puede ser verificada ya que el servidor ha recibido los datos de autentificación: USER_ID, EQ_ID, el identificador de mensaje MES_ID, el perfil de seguridad PRO_SEC que comprende el formato de la firma llegado el caso, y el contenido del mensaje DATA. Estos datos se pueden utilizar para verificar que el mensaje se ha firmado correctamente.

Descifrado del mensaje después de las verificaciones

Cuando el identificador del mensaje MES_ID y la autentificación del mensaje han sido verificados por el servidor SERV, este último procesa el campo que indica el perfil de seguridad que ha sido escogido por el cliente. Cuando este perfil indica que la cuenta del mensaje está cifrada, entonces el servidor emprende el descifrado de los datos útiles del mensaje gracias a la clave pública del equipo KApub. Los datos se descifran y se almacenan en una memoria o se emiten hacia una aplicación que procesa los datos.

Procesado del mensaje después de las verificaciones

Los datos útiles, una vez descodificados por el servidor, se transmiten a un componente APP que procesa funcionalmente el mensaje recibido. Este componente permite interpretar y gestionar el mensaje en el nivel de una capa de aplicación. Recíprocamente, en el lado del cliente, el componente APP permite procesar el contenido de los mensajes provenientes del servidor cuando estos últimos han sido validados y descifrados por el componente SEC_SW_C.

Ventajas

El método de la invención permite establecer una comunicación de manera securizada en forma de preguntas/respuestas entre un cliente y un servidor sin tener que gestionar los estados de una comunicación, es decir de las sesiones entre las entidades comunicantes. Así, la invención permite prescindir de un protocolo preliminar entre dos entidades de una red o de un enlace que tiene como objetivo preparar las condiciones de una comunicación securizada. Los medios de una comunicación securizada que intercambia datos en forma de preguntas/respuestas se pueden implementar respetando los principios de una arquitectura de tipo REST.

Por tanto, la invención permite prescindir de intercambios de datos tales como certificados o PKI aunque permitiendo una securización de los intercambios. La invención prescinde, por tanto, de una puesta en práctica de una infraestructura PKI que implica la gestión de certificados de autentificación. Otra de las ventajas de la invención es la de comportar un coste de despliegue reducido dado que la comunicación securizada se puede establecer entre dos entidades que se descubran por primera vez.

La solución de la invención permite suspender o revocar un equipo por parte del servidor. De manera idéntica, el servidor puede revocar o suspender una cuenta de usuario.

Otra de las ventajas de la invención es que el pirateo de la base de datos del servidor no permitirá que un tercero obtenga claves privadas de los equipos ya que la misma no almacena más que informaciones públicas.

Otra de las ventajas de la invención es la de permitir el fortalecimiento de la asociación entre un equipo y un usuario. En efecto, el procedimiento de la invención permite asociar en los intercambios, entre las entidades comunicantes, el identificador de usuario USER_ID y el identificador de un equipo EQ_ID. El equipo posee un identificador y un juego de claves asimétricas, y el usuario posee una cuenta de usuario que comprende por lo menos una contraseña y un identificador, con lo que el pirateo de un par de datos no permite acceder al servidor sin el otro par de datos.

REIVINDICACIONES

1. Procedimiento de comunicación entre dos entidades comunicantes, generando una primera entidad comunicante un mensaje de datos que comprende datos útiles y un encabezamiento de autentificación (TOKEN), constando dicho procedimiento de:

   - una generación de un identificador de mensaje (MES_ID) a partir de un parámetro dado y de una fecha y una inserción del identificador en un encabezamiento de autentificación (TOKEN);
   - una inserción de una pluralidad de datos de autentificación que comprenden por lo menos un identificador de usuario (USER_ID) y un identificador de equipo (EQ_ID) en el encabezamiento de autentificación (TOKEN);
   - una determinación y una inserción de un perfil de seguridad (PRO_SEC) en el encabezamiento de autentificación (TOKEN) que define las condiciones:
     - de cifrado de los datos útiles del mensaje emitido por la primera entidad comunicante;
     - de generación de una firma de datos del mensaje y del formato de dicha firma generada;
   - una inserción de los datos útiles en el mensaje a transmitir, de manera que la segunda entidad comunicante (SERV) tras la recepción de un mensaje de la primera entidad comunicante (CLIENTE) descodifica el encabezamiento de autentificación (TOKEN) para:
     - controlar el identificador de mensaje (MES_ID) para determinar si el mensaje ha sido emitido en un lapso de tiempo predefinido;
     - controlar el identificador del usuario (USER_ID) y el identificador del equipo (EQ_ID) comparando el valor de estos parámetros con datos almacenados en una memoria de la segunda entidad comunicante (SERV) con el fin de determinar si el equipo o el usuario ha sido suspendido o revocado;
     - controlar el parámetro de cifrado (P1, P3) del perfil de seguridad (PRO_SEC) del mensaje recibido para descifrar llegado el caso, los datos útiles con la clave privada de la segunda entidad comunicante (SERV);
     - controlar, llegado el caso, el parámetro de firma (P2, P4) del perfil de seguridad (PRO_SEC) del mensaje recibido con el fin de verificar llegado el caso la firma por medio de la clave pública (KApub) de la primera entidad comunicante (CLIENTE).

2. Procedimiento de comunicación según la reivindicación 1, el conjunto de datos a firmar comprende una combinación de los siguientes datos:

   - El identificador de mensaje (MES_ID);
   - El identificador de usuario (USER_EQ);
   - Una contraseña de una cuenta de usuario (MDP_ID);
   - El identificador del equipo (EQ_ID);
   - El perfil de seguridad (PRO_SEC);
   - Una información de encabezamientos o de un campo de datos de mensaje representativo del protocolo de transferencia de los datos útiles;
   - Los datos útiles (DATA).

3. Procedimiento de comunicación según la reivindicación 1, comprendiendo la primera entidad comunicante (CLIENTE) una memoria para almacenar una clave pública (KSpub) de una segunda entidad comunicante (SERVIDOR), caracterizado por que el perfil de seguridad (PRO_SEC) comprende:

   - un primer parámetro (P1) que indica la presencia o no de un cifrado de los datos útiles (DATA) efectuado a partir de la clave pública (KSpub) de la segunda entidad comunicante(SERVIDOR) y;
   - un segundo parámetro (P2) que indica la presencia o no de una firma de un conjunto de datos a firmar.

4. Procedimiento de comunicación según la reivindicación 1, comprendiendo la primera entidad comunicante (CLIENTE) una memoria para almacenar una clave pública (KSpub) de una segunda entidad comunicante

(SERVIDOR), caracterizado por que el perfil de seguridad (PRO_SEC) comprende:

- un primer parámetro (P1) que indica la presencia o no de un cifrado de los datos útiles (DATA) efectuado a partir de una clave simétrica y, llegado el caso, de la presencia de un cifrado de la clave simétrica a partir de la clave pública (KSpub) de la segunda entidad comunicante (SERVIDOR) y;
- un segundo parámetro (P2) que indica la presencia o no de una firma de un conjunto de datos a firmar.

5. Procedimiento de comunicación según una cualquiera de las reivindicaciones 3 a 4, caracterizado por que el perfil de seguridad (PRO_SEC) comprende:

- Un tercer parámetro (P3) que indica la presencia o no de un cifrado efectuado a partir de la clave pública (KApub) de la primera entidad comunicante (CLIENTE) bien de los datos útiles o bien de una clave simétrica y;
- Un cuarto parámetro (P4) que indica la presencia o no de una firma de un conjunto de datos a firmar,

de por lo menos un mensaje que debe ser emitido por una segunda entidad comunicante (SERVIDOR) como respuesta a un mensaje recibido de la primera entidad comunicante (CLIENTE).

6. Procedimiento de comunicación según la reivindicación 5, caracterizado por que el servidor comprende medios de acceso a la memoria que almacena los datos correspondientes a los identificadores de clientes (USER_ID) y a los identificadores de equipos (EQ_ID) para revocar o suspender uno o varios equipo(s) o cliente(s).

7. Procedimiento de comunicación según una de las reivindicaciones 1 a 6, caracterizado por que comprende, previamente, la ejecución de un procedimiento de generación de una petición de inscripción (REQ_E), siendo generada dicha petición de inscripción por una primera entidad comunicante (CLIENTE) con destino a una segunda entidad comunicante (SERV), y caracterizado por que comprende:

- Una activación del procedimiento de inscripción (M1_ENROL_C);
- Una generación de una petición de inscripción (REQ_E) que consta de un identificador de un equipo (EQ_ID), un identificador del usuario (USER_ID), una contraseña del usuario (USER_MDP) y una clave pública (KApub) de la primera entidad comunicante (CLIENTE);
- Un cifrado de la petición con una clave pública (KSpub) de la segunda entidad comunicante (SERV) y una emisión de la petición de inscripción (REQ_E) por medio de una interfaz de comunicación con destino a la segunda entidad comunicante (SERV).

8. Procedimiento según la reivindicación 7, caracterizado por que comprende previamente:

- Una creación de una cuenta de usuario que comprende un identificador (USER_ID) y una contraseña (USER_MDP);
- El registro de los datos de dicha cuenta de usuario en una memoria de la segunda entidad comunicante (SERV);
- Una adquisición (ACQ_KSpub) de una clave pública (KSpub) de la segunda entidad comunicante (SERV) para la cual se emprende el procedimiento de inscripción desde la primera entidad comunicante (CLIENTE);
- Una generación de un par de claves asimétricas (KApub, KApriv) de la primera entidad comunicante (CLIENTE).

9. Procedimiento, caracterizado por que la segunda entidad comunicante (SERV) comprende:

- Una recepción de una petición de inscripción generada por un procedimiento de generación de una petición de inscripción (REQ_E) según una de las reivindicaciones 7 a 8;
- Un descifrado de los datos de la petición de inscripción (REQ_E) por medio de una clave privada (KSpriv) de la segunda entidad comunicante (SERV);
- Una comparación entre el identificador de usuario (USER_ID) recibido y la contraseña de usuario (USER_MDP) recibida, con datos de cuentas de cliente almacenados en una memoria de la segunda entidad comunicante (SERV);
- Un registro del identificador del equipo (EQ_ID) en una memoria de la segunda entidad comunicante (SERV);

- Un registro de la clave pública (KApub) de la primera entidad comunicante (CLIENTE) asociada al identificador del equipo (EQ_ID) en una memoria de la segunda entidad comunicante (SERV).

10. Procedimiento según la reivindicación 9, caracterizado por que la segunda entidad comunicante (SERV) comprende:

- un control de una fecha actual con una fecha de referencia;
- una generación de un mensaje con destino a la primera entidad comunicante (CLIENTE) que comprende un código específico que indica que se debe renovar un par de claves asimétricas;
- una recepción de una nueva petición de inscripción generada por la primera entidad comunicante según el procedimiento de una de las reivindicaciones 7 a 8.

11. Entidad comunicante caracterizada por que comprende por lo menos una memoria, un módulo de cálculo y una interfaz de comunicación para la ejecución de las etapas del procedimiento de comunicación según una cualquiera de las reivindicaciones 1 a 10 realizadas por una misma entidad.

12. Programa de ordenador que consta de un conjunto de instrucciones para la puesta en práctica del procedimiento de comunicación de una cualquiera de las reivindicaciones 1 a 10.

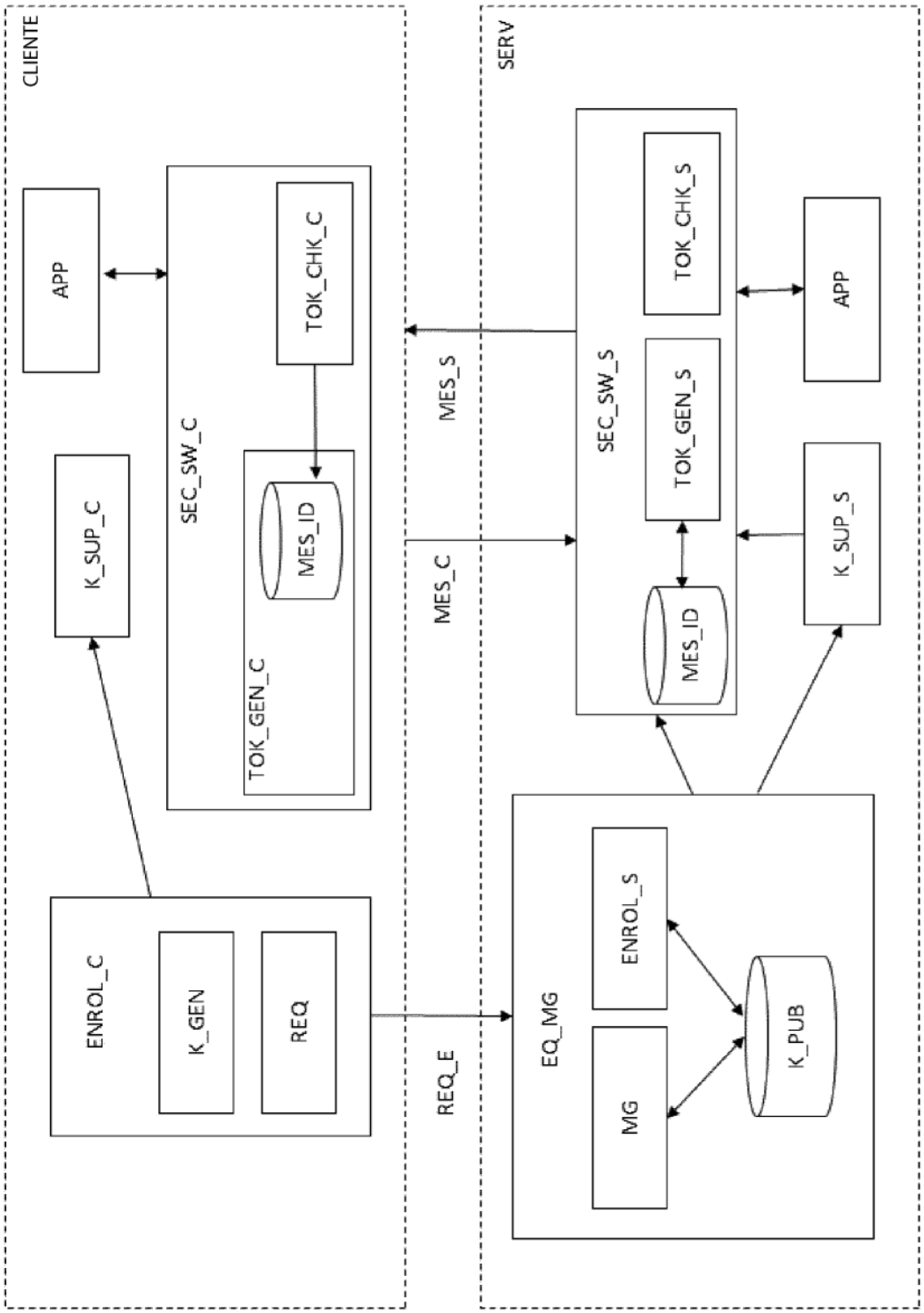
CLIENTE
APP
SEC_SW_C
TOK_CHK_C
TOK_GEN_C
MES_ID
K_SUP_C
ENROL_C
K_GEN
REQ
MES_S
MES_C
REQ_E
SERV
SEC_SW_S
TOK_CHK_S
TOK_GEN_S
MES_ID
APP
K_SUP_S
EQ_MG
ENROL_S
MG
K_PUB

FIG. 1

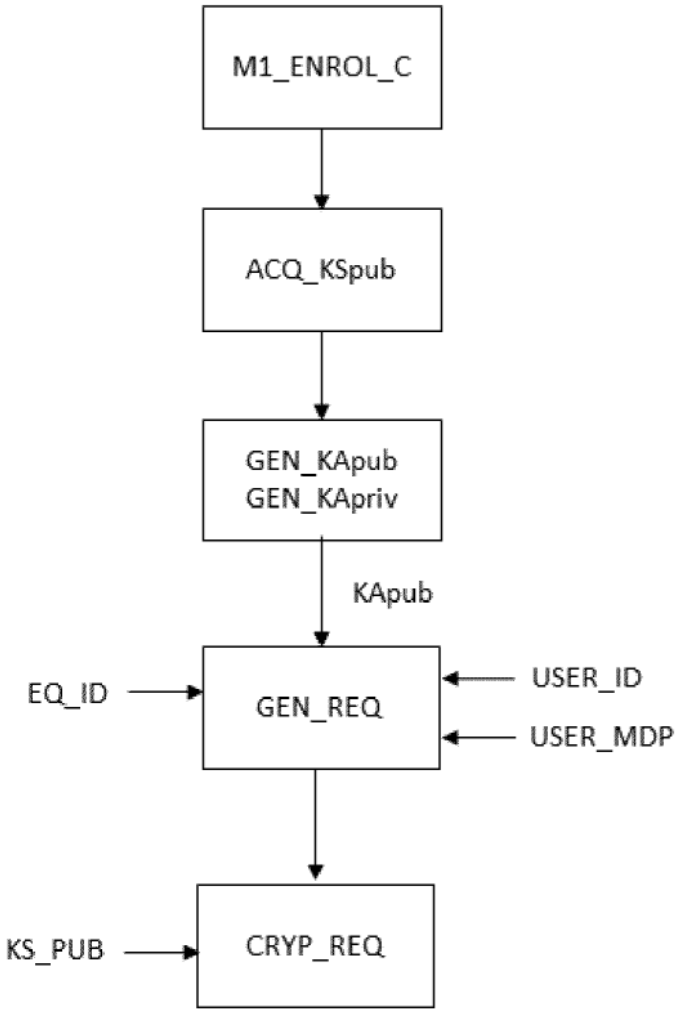
M1_ENROL_C
ACQ_KSpub
GEN_KApub
GEN_KApriv
KApub
EQ_ID
GEN_REQ
USER_ID
USER_MDP
KS_PUB
CRYP_REQ

FIG. 2A

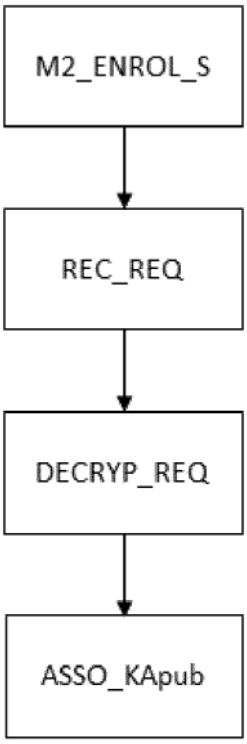
M2_ENROL_S
REC_REQ
DECRYP_REQ
ASSO_KApub

FIG. 2B

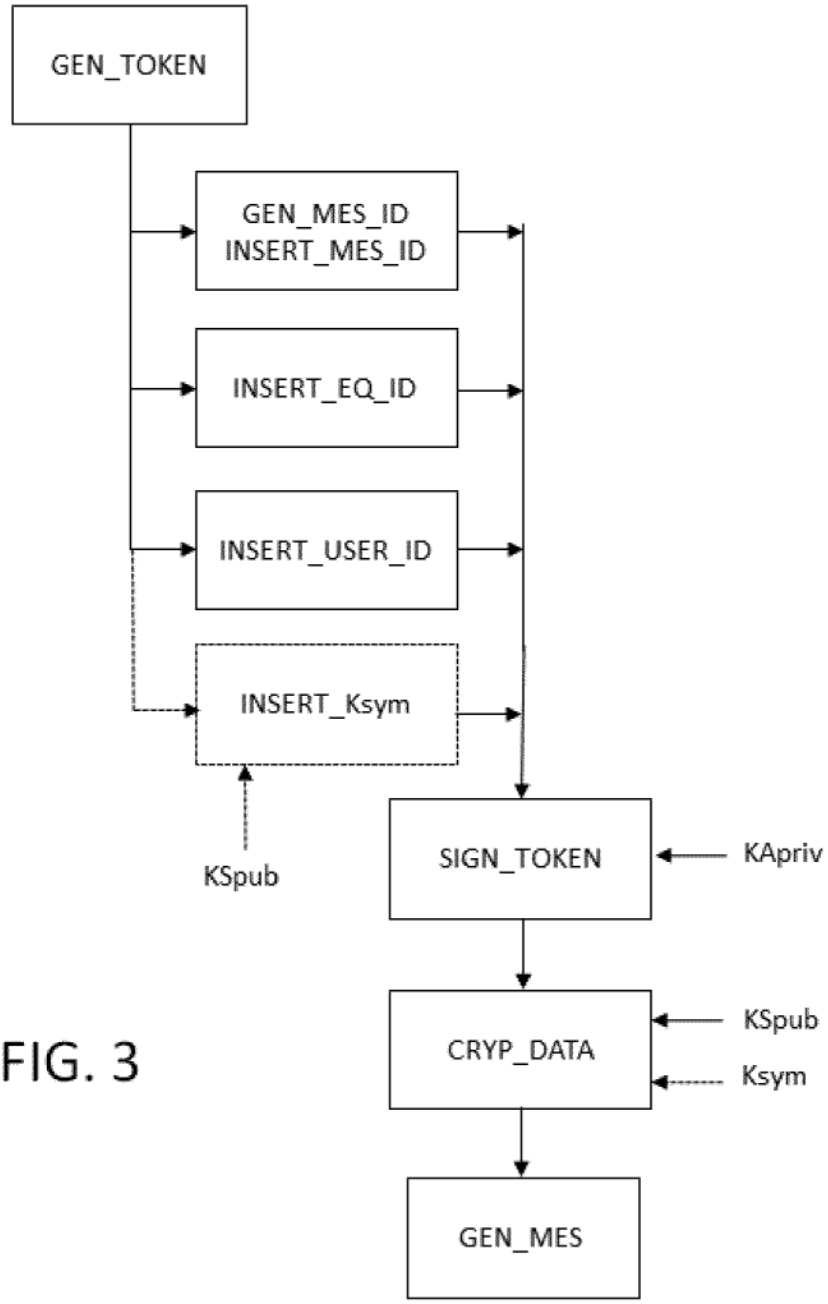
GEN_TOKEN
GEN_MES_ID
INSERT_MES_ID
INSERT_EQ_ID
INSERT_USER_ID
INSERT_Ksym
KSpub
SIGN_TOKEN
KApriv
CRYP_DATA
KSpub
Ksym
GEN_MES

FIG. 3