(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 788 976**

(21) Número de solicitud: 202030772

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) PATENTE DE INVENCIÓN CON EXAMEN B2

(22) Fecha de presentación:

24.07.2020

(43) Fecha de publicación de la solicitud:

23.10.2020

Fecha de modificación de las reivindicaciones:

19.01.2021

Fecha de concesión:

09.03.2022

(45) Fecha de publicación de la concesión:

16.03.2022

(73) Titular/es:

VEGA CRESPO, José Agustín Francisco Javier (50.0%)
C/ Señora Sergia, 41
28250 TORRELODONES (Madrid) ES y
CARRILLO VERDÚN, José Domingo (50.0%)

(72) Inventor/es:

VEGA CRESPO, José Agustín Francisco Javier y
CARRILLO VERDÚN, José Domingo

(74) Agente/Representante:

DÍAZ DE BUSTAMANTE TERMINEL, Isidro

(54) Título: **SISTEMA PARA EL CIFRADO Y AUTENTICACIÓN DE COMUNICACIONES CON AUTENTICACIÓN MUTUA DE LOS COMUNICANTES**

(57) Resumen:

Sistema para el cifrado y autenticación de comunicaciones con autenticación mutua de los comunicantes que, aplicable entre dos partes que intercambian mensajes soportados por una red de comunicaciones donde están identificadas de forma inequívoca, comprende procesos soportados por respectivas aplicaciones de autenticación de que dispone cada parte en un dispositivo hardware/software, las cuales, al menos, comprenden: un Identificador (Id) de la Aplicación de Autenticación (AA); una Clave de Cifrado(CC) de cada una de las partes; un generador de valores aleatorios para cifrar y autenticar mensajes Mx; un algoritmo de cifrado y una función resumen, que comparte con el resto de las partes del sistema, que les permite cifrar y descifrar los mensajes que se envían/reciben y la obtención de valores resumen.

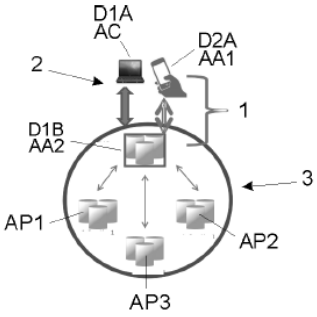

FIG. 1

ES 2 788 976 B2

DESCRIPCIÓN

SISTEMA PARA EL CIFRADO Y AUTENTICACIÓN DE COMUNICACIONES CON AUTENTICACIÓN MUTUA DE LOS COMUNICANTES

OBJETO DE LA INVENCIÓN

La invención, tal como expresa el enunciado de la presente memoria descriptiva, se refiere a un sistema para el cifrado y autenticación de comunicaciones con autenticación mutua de los comunicantes aportando, a la función a que se destina, ventajas y características, que se describen en detalle más adelante, que suponen una mejora del estado actual de la técnica.

Más concretamente, el objeto de la invención se centra en un sistema en el que, al menos, dos partes se intercambian mensajes de comunicación electrónica mediante equipos informáticos haciendo uso de un protocolo de autenticación mutua de forma que al final del proceso quedan inequívocamente identificadas entre ellas y dicha autenticación mutua también les sirve para autenticar y confirmar la autoría de los datos que se intercambian a lo largo del dialogo que llevan a cabo, normalmente con el fin de realizar una operación entre ellos.

CAMPO DE APLICACIÓN DE LA INVENCIÓN

El campo de aplicación de la presente invención se enmarca en el área de las tecnologías de la información, dentro del sector de la ciberseguridad, concretamente en el de la autenticación de las comunicaciones que se llevan a cabo en el ciberespacio.

ANTECEDENTES DE LA INVENCIÓN

Está claro que en la sociedad actual las comunicaciones juegan un papel fundamental en nuestra actividad diaria y de su seguridad dependerá el que estas actividades puedan ser realizadas correctamente.

Son muchas las vulnerabilidades que se pueden presentar en cualquier tipo de comunicación y más cuando hay tantas personas dedicadas a hacer negocio explotando sus puntos débiles.

Según un informe elaborado por la consultora Marsh & McLennan junto a Mandiat, el importe económico de los delitos cibernéticos en 2018 se cifró en unos 600.000 millones de euros (un 33% más que en 2016). Más del 90% de los incidentes cibernéticos fueron causados por técnicas de ingeniería social, principalmente ataques de *phishing* que suplantan la identidad del emisor o destinatario de una comunicación para cometer el fraude. Y el *phishing* se puede evitar si antes de realizar la comunicación se somete a un proceso de autenticación mutua a su emisor y destinatario, ya que así se elimina la posibilidad de la suplantación de identidad.

¿Qué es lo importante de una comunicación segura?

Para el emisor lo importante es que el mensaje una vez emitido llegue ciertamente a sus destinatarios, y únicamente a ellos, y que en el camino dicho mensaje no sea manipulado.

Para el destinatario es fundamental el saber quién es su emisor real y que el contenido original del mensaje no ha podido ser manipulado.

Si se quieren ver cumplidas estas necesidades del emisor y del destinatario de un mensaje dicho mensaje deberá haber sido sometido a una autenticación basada en un sistema de autenticación de mensajes en el que:

- Para saber que una comunicación ciertamente le ha llegado a su destinatario “su protocolo de transmisión deberá contemplar una respuesta del destinatario al emisor” en la que se confirme que ciertamente le llegó el mensaje enviado, asegurándose de que ciertamente es el destinatario quién envía dicha respuesta.
- Si queremos que el mensaje únicamente le llegue a su destinatario será necesario que “la transmisión sea realizada mediante un algoritmo y clave de cifrado fuertes” común al emisor y receptor que únicamente sea conocido por ellos.
- Para que el destinatario sepa que el mensaje no ha podido ser manipulado habrá que añadirle algo que sirva para verificar su integridad. Una forma de hacerlo en una transmisión puede ser “incorporando al mensaje una función resumen (hash)” que proporcione un mismo y único valor preciso para un mensaje determinado.
- Si en una comunicación se quiere que queden correctamente identificados su emisor y su destinatario será necesario que “se lleve a cabo entre ellos una autenticación mutua” que es aquella que permite a ambas partes identificarse recíprocamente sin que quede lugar a dudas de quién es cada uno de ellos. Para ello se seguirá un protocolo de intercambio de

mensajes, que tendrá como finalidad dicha identificación mutua.

La mayor o menor vulnerabilidad de un sistema de autenticación de comunicaciones dependerá, en gran parte, del grado de cumplimiento de los puntos anteriormente citados.

Casi todos los sistemas de comunicación existentes los aplican parcialmente y muy pocos aplican todos ellos.

Actualmente existen ya en el mercado una gran variedad de sistemas de autenticación de comunicaciones, que utilizan distintos medios y procedimientos, para lograr la autenticación de comunicaciones entre dos partes que dialogan de una forma no presencial.

Hasta hace relativamente poco tiempo estos sistemas sólo autenticaban al emisor del mensaje y lo hacían (y todavía se sigue haciendo en demasiados casos) utilizando un identificador del cliente y una clave de valor fijo (PIN). Esta forma de identificarse es bastante poco eficaz ya que cualquier delincuente puede estar suplantando al destinatario (la empresa) consiguiendo así hacerse con los datos del emisor para posteriormente utilizarlos en su beneficio. Por otro lado estos datos que se están enviando para identificar al emisor ya no son suficientes pues muchos de ellos ya están siendo conseguidos fraudulentamente y vendidos a delincuentes. Está claro que no se puede confiar en contraseñas estáticas.

En la actualidad son ya muchas empresas las que complementan el sistema de autenticación anterior con el envío de un SMS con una clave OTP (*One Time Password*) al teléfono móvil del usuario para que se la reenvíe a la empresa con lo que, en principio, la empresa se asegura de que el que está solicitando operar dispone del móvil del usuario y, por lo tanto, es el usuario. Esta forma de actuar estaría en línea con lo que los estándares internacionales están demandando y que es una autenticación multifactor. El problema es que se estén utilizando los SMS que tienen el inconveniente de que su emisor no tiene forma de verificar si la persona que lo recibe es el destinatario correcto dada la facilidad con la que puede haber sido interceptado por un delincuente.

Existen otros sistemas de autenticación de mensajes, con la finalidad de autenticar accesos para la operativa online de una empresa, que usan una o dos claves OTP (claves de un único uso). En este tipo de sistemas si un usuario sufre un ataque de *Phishing/Pharming* en tiempo real un delincuente puede hacerse con la primera clave OTP y, usándola antes de que

caduque su validez, puede suplantar a dicho usuario.

También existen sistemas que usan dos claves OTP y una fija o tres claves OTP. Todos ellos pueden ser objeto fácil de un ataque *Man In The Middle* si en sus comunicaciones no hacen uso de, al menos, un segundo canal (físico o lógico) de comunicación.
Todos estos sistemas de autenticación tienen en común el que son utilizados por personas que, en la mayor parte de los casos, se ven obligadas a memorizar contraseñas y a teclearlas sin cometer errores. Además deben tomar precauciones para que nadie les engañe y se hagan con ellas.

Según estudios de acreditadas empresas, muchos de los fraudes que cometen los delincuentes que acceden a información dentro de un sistema informático tienen su origen en un previo descuido o engaño de un usuario con acceso a dicho sistema. El delincuente por medio del malware disponible y, generalmente, de la ingeniería social consigue hacerse con las credenciales del usuario y lo suplanta para acceder al sistema.

Existe un consenso generalizado sobre el hecho de que es la intervención del usuario en su proceso de autenticación la que, normalmente, origina el eslabón más débil por el que se puede romper la solidez de dicho proceso. Por esta razón es por la que los nuevos procesos de autenticación deberán intentar automatizar todo aquello que actualmente se le suele pedir que haga el usuario. Así, “minimizando la participación del usuario en los procesos de autenticación, se podría conseguir la mejora de su usabilidad y disminuir el fraude”.

El objetivo de la presente invención es, pues, el desarrollo de un sistema de intercambio de mensajes que permita solventar los problemas señalados incorporando como características diferenciadoras las soluciones citadas anteriormente, es decir:

- Que las comunicaciones hagan uso de un algoritmo y clave de cifrado fuertes que garanticen la integridad y confidencialidad de lo comunicado.
- Que las comunicaciones incorporen al mensaje una función resumen (hash) que permita verificar su integridad.
- Que su protocolo de comunicación contemple una respuesta del destinatario al emisor que asegure al emisor que el destinatario ha recibido la comunicación y no pueda darse un posterior repudio tanto de haberla emitido como de haberla recibido.
- Que el protocolo de intercambio de mensajes entre las partes realice una autenticación

mutua entre emisor y destinatario que garantice al destinatario quién es el emisor y al emisor quién es el destinatario.

- Que sus comunicaciones hagan uso de, al menos, un segundo canal de comunicación que en caso de interceptación de las comunicaciones de uno de ellos permita hacer verificaciones en el otro que puedan detectar manipulaciones de la información, impidiendo de esta forma fraudes del tipo "*Man In The Middle"*.
- Que su protocolo de comunicación minimice la intervención del usuario en el proceso de comunicación evitando sus errores y posibles engaños de ingeniería social que faciliten el fraude, especialmente los de tipo *Phishing*.

EXPLICACIÓN DE LA INVENCIÓN

El sistema para el cifrado y autenticación de comunicaciones con autenticación mutua de los comunicantes que la invención propone permite alcanzar satisfactoriamente los objetivos anteriormente señalados, estando los detalles caracterizadores que lo hacen posible y que lo distinguen convenientemente recogidos en las reivindicaciones finales que acompañan a la presente descripción.

Lo que la invención propone, tal como se ha apuntado anteriormente, es un sistema en el que dos partes se intercambian mensajes de comunicación electrónica mediante equipos informáticos haciendo uso de un protocolo de autenticación mutua de forma que al final del proceso quedan inequívocamente identificadas las partes entre sí y también queda autenticada la información que viaja en los mensajes intercambiados.

El sistema de autenticación se aplica, principalmente, a un diálogo entre dos Partes (Parte A y Parte B) que se intercambian dos o más mensajes con objeto de resolver una operación con interés para ambas Partes. El diálogo está soportado por el sistema de autenticación en el que están integradas e identificadas de forma inequívoca dichas partes que se comunican entre ellas por uno o más canales de comunicación.

Dicho Sistema de Autenticación está compuesto por procesos soportados por las respectivas Aplicaciones de Autenticación de que dispone cada una de las Partes integradas en el Sistema de Autenticación.

Para ello:

Cada Parte dispone de un dispositivo hardware/software, en el que se ejecuta una Aplicación de Autenticación (AA) que contiene el software que implementa su forma de actuar de acuerdo con el procedimiento de autenticación mutua.

Cada Parte dispone de una Aplicación de Autenticación que contiene:

-un Identificador (Id) que identifica a la Aplicación de Autenticación (AA) de forma inequívoca frente al resto de Aplicaciones de Autenticación integradas en el Sistema de Autenticación;
-el Identificador de cada una de las Aplicaciones de Autenticación de las otras Partes que puedan llegar a ser su interlocutor dentro del Sistema de Autenticación;
- uno o más canales de comunicación con que las aplicación de autenticación se intercambian los mensajes;

-la Clave de Cifrado (CC) de cada una de las Partes que pueda llegar a ser su interlocutor, siendo éstos valores diferentes para cada pareja de Partes.

Ejemplo:
Las Partes A, B, C se pueden relacionar todas entre ellas recíprocamente:

Para ello, cada Parte deberá de disponer de los valores:
A - IdA,
IdB - CCAB;
IdC - CCAC
B - IdB,
IdA - CCAB;
IdC - CCBC
C - IdC,
IdB - CCBC;
IdA - CCAC
Así, para los diálogos entre A y B necesitan que sus Aplicaciones de Autenticación compartan sus IdA, IdB y el valor CCAB;

- un generador de Valores Pseudoaleatorios que serán usados para cifrar y/o autenticar

mensajes Mx;

- un algoritmo de cifrado, que comparte con el resto de las Partes del Sistema, que les permite cifrar y descifrar los mensajes que se envían/reciben;

- opcionalmente, cuando una de las partes es una persona física, un Código de Activación (CA) específico de cada Aplicación de Autenticación, AA, que, por razones de seguridad, autentique a dicha persona frente a la AA y deba ser usado para activar dicha AA de forma que nadie, excepto dicha persona, pueda hacer uso de la AA ni de sus datos (entre ellos el CC) sin su conocimiento.

Las tareas que ejecutarán las Partes A y B con sus Aplicaciones de Autenticación son:

- Parte A

Inicia el procedimiento para un diálogo con la Parte B, en el que se van a intercambiar tres mensajes, y para ello, haciendo uso de su Dispositivo y su Aplicación de Autenticación AAA:

- Genera y guarda cuatro Valores Pseudoaleatorios, CCM2, VAM2 y CCM3, VAM3 a usar como Claves de Cifrado (CCMx) de los mensajes y Valores de Autenticación (VAMx) en los mensajes M2 y M3 respectivamente. Todos estos valores generados tendrán un tiempo de validez determinado que será controlado en su proceso de uso. La cantidad de valores pseudoaleatorios a generar dependerá de cuantos mensajes se vayan a intercambiar a lo largo del diálogo entre las Partes de forma que haya dos valores a usar por cada mensaje M2 y sucesivos.

- Obtiene el Timestamp del momento (TS); prepara la información a enviar conteniendo, al menos, los valores IdB, IdA, TS, CCM2, VAM2, CCM3, VAM3 y DATOS1, donde DATOS1 contendrá información que se desee comunicar a la Parte B; aplica a ésta información una función resumen determinada (función hash tipo Secure Hash Algorithm o cualquier otro algoritmo similar) obteniendo un Valor Resumen de la información a transmitir en el mensaje M1, VRM1; cifra con CCAB, obteniendo CCAB(TS, CCM2, VAM2, CCM3, VAM3, DATOS1, VRM1).

- Envía a la Parte B un mensaje M1 conteniendo, entre otros posibles, los datos: IdB; IdA; CCAB(TS, CCM2, VAM2, CCM3, VAM3, DATOS1, VRM1).

Opcionalmente, por su interés para la operativa y controles, también podrá viajar cifrado por CCAB el identificador del emisor del mensaje en la red de comunicación que soporta el diálogo.

- Parte B

Continúa con el procedimiento para un diálogo con la Parte A, en el que se van a intercambiar tres mensajes, y para ello, haciendo uso de su Dispositivo y su Aplicación de Autenticación AAB:

a) Recibe el mensaje M1 y continúa con el procedimiento de autenticación del diálogo iniciado. Para ello:

-Verifica el Identificador de Parte A.

-Descifra con CCAB el CCAB(TS, CCM2, VAM2, CCM3, VAM3, DATOS1, VRM1); aplica la misma función resumen a los mismos valores recibidos y obtiene el Valor Resumen que debe tener el VRM1 recibido y si coincide el Valor Resumen calculado con el recibido es que el descifrado ha sido realizado correctamente y el mensaje no ha sido manipulado. Esto quiere decir que el valor CCAB es el que se usó para cifrar y por lo tanto el que creó el mensaje y realizó el cifrado ha sido la Parte A, ya que sólo ella conoce dicho valor. Además queda garantizada la integridad y confidencialidad de la información recibida. También, opcionalmente, se controlará que el Timestamp TS recibido es igual o mayor que el del último mensaje tratado y que está dentro de un rango de valores convenido.

Nota 1: así, está claro que el creador del mensaje y el que ha iniciado el diálogo es la Parte A.

b) La Parte B, una vez recibido el M1 y verificado que viene de la Parte A, prepara y envía, a la Parte A, un mensaje M2, continuando con el procedimiento de autenticación del diálogo ya iniciado. Para ello:

- Guarda los valores CCM2, VAM2, CCM3, VAM3 para su posterior uso.
- Compone el mensaje (TS2, VAM2, DATOS2), con el Timestamp del momento TS2 y los DATOS2 a enviar, y lo cifra con CCM2.
- Envía a la Parte A (IdA) un mensaje M2 conteniendo, entre otros posibles valores, los de:

IdA; IdB; CCM2(TS2, VAM2 DATOS2).

Nota 2: siguiendo con el razonamiento de la Nota 1, lo que sí sabemos es que el que reciba el mensaje, si no es la Parte A, no va a poder descifrarlo pues no conoce el valor CCM2 y, por lo tanto, no conocerá los datos enviados a la Parte A y el mensaje sólo

tendrá una respuesta coherente y válida si es que ciertamente lo acaba recibiendo la Parte A.

Parte A

a) Recibe de Parte B el mensaje M2 : IdA; IdB; CCM2(TS2, VAM2, DATOS2) y continúa con el procedimiento de autenticación del diálogo ya iniciado. Para ello:

-Verifica el Identificador de Parte B.

-Descifra con CCM2 la información del M2 para obtener el VAM2 y verificar su coincidencia con el enviado en el M1 con lo que se asegura de que el descifrado ha sido correcto y que el M2 es la respuesta al M1 enviado ya que contiene el valor VAM2, con lo que queda autenticado el mensaje. Como únicamente es la Parte B la que conoce el valor CCM2 con el que llegó cifrado el mensaje M2, queda asegurada la autenticidad de la Parte B como creador del mensaje y, de ésta forma, la Parte A sabe que ciertamente está dialogando con la Parte B, completándose el proceso de autenticación mutua. Al viajar el mensaje cifrado también queda garantizada su integridad y confidencialidad. El hecho de que la secuencia de los mensajes venga fijada por la presencia en el mensaje de los valores pseudoaleatorios VAMx, y no por un valor fijo predeterminado que establezca un orden en la secuencia de los mensajes, fortalece la seguridad del cifrado ya que la mayoría de las técnicas usadas para romper los cifrados lo que hacen es buscar la existencia de valores fijos presentes en el texto cifrado.

b) Con el fin de que la Parte B sepa con seguridad que el M2 llegó a la Parte A y que, por lo tanto, el proceso de autenticación mutua ha sido realizado correctamente, será necesario que la Parte A envíe a la Parte B un M3 confirmando la recepción del M2, sabiendo la Parte B que, siguiendo el procedimiento objeto de la invención, la Parte A responderá únicamente si ha recibido el mensaje M2 y comprobado que para su cifrado se usó el CCM2 enviado en el M1. Siendo así:

- Compone el mensaje (TS3, VAM3, DATOS3), con el TS3 del momento y los DATOS3 a enviar, y lo cifra con CCM3.
- Envía a la Parte B (IdB) un mensaje M3 conteniendo, entre otros posibles valores, los de: IdB; IdA; CCM3(TS3, VAM3, DATOS3).

De esta forma cuando la Parte B reciba el mensaje lo descifre con CCM3 y verifique el VAM3 tendrá la seguridad de que es la Parte A su emisor y de que el mensaje M2 ciertamente fue recibido por la Parte A y ésta es su respuesta, ya que, siguiendo el procedimiento de

autenticación objeto de la invención, la Parte A no hubiera enviado éste mensaje si no hubiera recibido previamente el M2 cifrado con el valor CCM2 correcto, y ningún otro puede haberlo creado pues únicamente la Parte A es la que dispone de la clave de cifrado CCM3.

Así, el procedimiento de autenticación mutua queda completado desde el punto de vista de quienes han sido los creadores de los mensajes intercambiados en el diálogo, Parte A y Parte B, y con la seguridad de la autenticidad de los datos, su integridad y su confidencialidad; queda autenticado, acreditado, que la información enviada por la Parte A en el mensaje M1 sí que le llegó a la Parte B y que la recibida en el M2 es justamente su respuesta al M1, así como que el M2 le llegó a la Parte A y que el M3 es la respuesta al M2; con lo que ya ninguna de las dos Partes puede alegar el desconocimiento o repudio de la operación.

En el caso en que la operativa a autenticar requiera que la Parte A sepa que su M3 ciertamente llegó a la Parte B será necesario que la Parte B envíe a la Parte A un nuevo mensaje M4 y para ello, en éste caso, se habrá generado y transmitido al inicio otros valores pseudoaleatorios CCM4 y VAM4. Y así sucesivamente.

La misma forma de proceder permitirá llevar a cabo un diálogo iniciado por la Parte B que tiene como destinatario la Parte A.

En todos los mensajes, de manera opcional, por su interés para su posterior auditoría y gestión, también podrá viajar cifrado un valor que agrupe y diferencie todos los mensajes que pertenecen a un mismo diálogo.

En todos los mensajes, de manera opcional, por su interés para la operativa y controles, también podrá viajar cifrado el identificador del emisor del mensaje en la red de comunicación que soporta el diálogo y el valor resumen resultado de aplicar una función resumen (función hash tipo SHA, *Secure Hash Algorithm* o algoritmo similar) al grupo de datos que, viajando en el mensaje, interese asegurar su integridad, incluidos los IdA e IdB.

Opcionalmente, las Partes pueden disponer de otros valores, además del CC, compartidos con cada uno de sus posibles interlocutores, valores diferentes para cada uno de estos posibles interlocutores, y que podrán ser usados dentro de otras operativas diferentes que puedan ser llevadas a cabo entre ellos. Como un ejemplo posible, entre muchos otros, podría ser el caso de una operativa que permita guardar almacenada toda la información que una

Parte quiera compartir con otra Parte, y únicamente con dicha Parte, cifrada con un segundo valor que comparten únicamente dichas dos Partes. Así, siguiendo con un ejemplo, las dos Partes podrían compartir todas las informaciones intercambiadas entre ellos en sus diálogos, autenticados según el procedimiento, habiendo sido guardadas (almacenadas) después de haber sido cifradas con el segundo valor que comparten. Únicamente ellas conocen dicho valor de cifrado y nadie más podrá disponer de dicha información.

En el sistema de autenticación, objeto de la invención, se lleva a cabo una autenticación mutua entre las Aplicaciones de Autenticación que a su vez autentica los mensajes que se intercambian. En el caso de que una de las Aplicaciones esté siendo usada por una persona física lo que no se puede asegurar es quién es el que está usando dicha Aplicación de Autenticación y, por lo tanto, quién es el verdadero emisor y destinatario final de los mensajes intercambiados. Inicialmente el hecho de que un usuario disponga de la Aplicación ya es un primer factor indicador de que es su verdadero usuario. Dado que es fácil el robo de un dispositivo con su Aplicación de Autenticación instalada lo habitual es que la Aplicación obligue a su usuario a aportar uno o más factores de autenticación que lo identifiquen. El más habitual es el Código de Activación CA que la Aplicación necesita para ponerse en funcionamiento.

Para que la autenticación de la Parte/persona que interviene en el proceso no dependa exclusivamente del conocimiento del Código de Activación de la aplicación de autenticación y de la posesión del dispositivo con su Aplicación de Autenticación (doble Factor de Autenticación, 2FA), se puede definir un nuevo factor, elemento físico o lógico independiente de la AA, tal que dicho elemento sea el que contenga una información sin la cual dicho proceso de autenticación no pueda darse por finalizado de forma correcta. Este elemento será conocido como el Tercer Factor de Autenticación necesario para la realización de una operación de autenticación (3FA).

Para incorporar éste 3FA al procedimiento de autenticación descrito, se convendrá en que:

- cuando la Parte B crea el mensaje M2 a enviar a la Parte A (persona física), en lugar de enviar el valor VAM2 recibido, enviará un valor 3FAVAM2 que se obtendrá complementando el valor VAM2 con el valor 3FA que tiene la Parte B para sus diálogos con la Parte A cuando quiere que la Parte A (persona) haga uso del tercer factor de autenticación. La forma como se “complementa” el VAM2 con el 3FA podrá ser una cualquiera de todas aquellas que partiendo de los dos citados valores generen un único

valor resultante, 3FAVAM2;

- cuando Parte A (persona) recibe de Parte B el mensaje M2 deberá aportar a su Aplicación de Autenticación éste valor 3FA, haciendo uso del tercer elemento que posee, para complementar el VAM2 enviado en el M1 y obtener el 3FAVAM2 a comparar con el valor 3FAVAM2 que llega en el M2 y así, si coinciden, poder tratar correctamente el mensaje M2.

Operando de ésta forma el procedimiento de autenticación sólo puede ser finalizado correctamente si el Destinatario del mensaje M2 dispone de un Tercer Factor de Autenticación con lo que ello supone en cuanto a potenciar el nivel de seguridad del proceso de autenticación mutua.

Opcionalmente, de forma similar, se puede hacer que el destinatario del mensaje M1 o M3 necesite también de un tercer factor de autenticación para poder continuar con el procedimiento de autenticación.

Esta forma de operar permite que el procedimiento de autenticación pueda ser usado, según interese, en el modo de dos factores de autenticación (2FA) o en éste nuevo modo que hace uso de un tercer factor de autenticación (3FA).

Dependiendo de la aplicación que se esté dando al Procedimiento de Autenticación habrá otras formas de aplicar el 3FA siempre que la ausencia de dicho 3FA impida finalizar correctamente el proceso al que se aplique.

Opcionalmente, el procedimiento de autenticación descrito contempla posibles simplificaciones.

- Con el fin de disminuir el consumo de recursos por parte de las Aplicaciones de Autenticación se puede acordar que los mensajes M2 y sucesivos, empleados en un mismo diálogo entre las Partes A y B, viajen sin cifrar con lo que ya no serán necesarios los valores CCM2 y CCM3 y tampoco las operaciones de cifrado y descifrado de dichos mensajes.

- Por su importancia en los posibles casos de uso del procedimiento de autenticación hay una simplificación del procedimiento de autenticación descrito que conviene destacar. Es el caso en el que sólo una de las Partes (Parte Central) tiene la capacidad de dialogar con todas las

demás Partes contempladas por el sistema que soporta sus diálogos, mientras que todos los demás, excepto ésta una, sólo pueden dialogar con dicha una (Parte Central).

En este caso, si suponemos que la Parte Central es la PC, cada una de ellas deberá de disponer de los valores:

A - IdA,
IdPC - CCA
B - IdB,
IdPC - CCB
C - IdC,
IdPC - CCC
PC - IdPC,
IdA - CCA;
IdB - CCB;
IdC - CCC

Como se puede ver, únicamente la Parte Central, PC, es la que debe tener las variables que le permiten dialogar con todas las otras Partes, aportando como ventaja el no tener que realizar la actividad de almacenar y mantener actualizadas todas las variables Id y CC de los posibles interlocutores de las Partes exceptuando en la Parte Central que sí debe disponer de ellos.

– En la implementación, las operaciones de cifrado y descifrado pueden hacer uso de un algoritmo de cifrado simétrico tipo AES, que consuman menos recursos que otros tipos de cifrado, y, preferentemente, con claves de cifrado CC y valores de autenticación VA de 16 Bytes (128 bites).

Estas simplificaciones pueden ser aplicadas todas juntas, al mismo tiempo, o sólo aquellas que puedan resultar de interés en un caso concreto.

- Procedimiento de autenticación simplificado preferente.

Se obtiene aplicando, al procedimiento de autenticación mutua descrito, todas las simplificaciones expuestas anteriormente.

En él, para los diálogos entre A y B ambas Partes necesitan compartir sus Identificadores, dentro del sistema de autenticación, IdA y IdB y el valor CCA.

A partir de ahora, en ésta descripción del Procedimiento Simplificado y aplicable de forma genérica para cualquier comunicación entre la Parte Central (Parte B) y cualquier otra de las Partes A, se mencionaran genéricamente como IdA, IdB y CC. Así:
Parte A - IdA,
IdB - CC;
Parte B - IdB,
IdA - CC.

Las tareas que ejecutarán las Partes A y B con sus Aplicaciones de Autenticación son:

- Parte A

Inicia el procedimiento para un diálogo con la Parte B, en el que se van a intercambiar tres mensajes, y para ello, haciendo uso de su Dispositivo y su Aplicación de Autenticación AAA:

- Genera y guarda dos Valores Pseudoaleatorios, VAM2 y VAM3 a usar como Valores de Autenticación (VAMx) en los mensajes M2 y M3 respectivamente. Todos estos valores generados tendrán un tiempo de validez determinado que será controlado en su proceso de uso. La cantidad de valores pseudoaleatorios a generar dependerá de cuantos mensajes se vayan a intercambiar a lo largo del diálogo entre las Partes de forma que haya un valor a usar por cada mensaje M2 y sucesivos.
- Obtiene el Timestamp del momento TS; prepara la información a enviar conteniendo, al menos, los valores IdA, IdB, TS, VAM2, VAM3 y DATOS, donde DATOS contendrá información que se desee comunicar a la Parte B; aplica a ésta información una función resumen (función hash tipo Secure Hash Algorithm o cualquier otro algoritmo similar) obteniendo un Valor Resumen de la información a transmitir en el mensaje M1, VRM1; cifra con CC, obteniendo CC(TS, VAM2, VAM3, DATOS, VRM1).
- Envía a la Parte B un mensaje M1 conteniendo, entre otros posibles, los datos: IdB; IdA; CC(TS, VAM2, VAM3, DATOS, VRM1).
Opcionalmente, por su interés para la operativa y controles, también podrá viajar cifrado por CC el identificador del emisor del mensaje en la red de comunicación que soporta el diálogo.

- Parte B

Continúa con el procedimiento para un diálogo con la Parte A, en el que se van a intercambiar tres mensajes, y para ello, haciendo uso de su Dispositivo y su Aplicación de Autenticación AAB:

a) Recibe el mensaje M1 y continúa con el procedimiento de autenticación del diálogo iniciado. Para ello:

- Verifica el Identificador de Parte A.
- Descifra con CC el CC(TS, VAM2, VAM3, DATOS, VRM1); aplica la misma función resumen a los mismos valores recibidos y obtiene el Valor Resumen que debe tener el VRM1 recibido y si coincide el VRM1 calculado con el recibido es que el descifrado ha sido realizado correctamente. Esto quiere decir que el valor CC es el que se usó para cifrar y por lo tanto el que creó el mensaje y realizó el cifrado ha sido la Parte A, ya que sólo ella conoce dicho valor. Además queda garantizada la integridad y confidencialidad de la información recibida. También, opcionalmente, se controlará que el Timestamp TS recibido es igual o mayor que el del último mensaje tratado y que está dentro de un rango de valores convenido.

Nota 1: así, está claro que el creador del mensaje y el que ha iniciado el diálogo es la Parte A.

b) La Parte B, una vez recibido el M1 y verificado que viene de la Parte A, prepara y envía, a la Parte A, un mensaje M2, continuando con el procedimiento de autenticación del diálogo ya iniciado. Para ello:

- Guarda los valores VAM2, VAM3, para su posterior uso.
- Compone el mensaje IdA, IdB, TS2, DATOS, VAM2, con el TS2 del momento y los DATOS a enviar, y calcula su valor resumen VRM2 aplicando una función resumen determinada.
- Envía a la Parte A (IdA) un mensaje M2 conteniendo, entre otros posibles valores, los de: IdA, IdB, TS2, DATOS, VRM2.

Nota 2: siguiendo con el razonamiento de la Nota 1, lo que sí sabemos es que el que reciba el mensaje, si no es la Parte A, desconoce el valor VAM2 y, por lo tanto, no podrá recalcular el VRM2 correcto y el mensaje sólo tendrá una respuesta coherente y válida si ciertamente lo acaba recibiendo la Parte A.

- Parte A

c) Recibe de Parte B el mensaje M2 : IdA; IdB; TS2, DATOS, VRM2 y continúa con el

procedimiento de autenticación del diálogo ya iniciado. Para ello:

-Verifica el Identificador de Parte B.

-Recalcula el valor de VRM2 teniendo en cuenta los datos recibidos IdA, IdB, TS2, DATOS y el valor VAM2 enviado en el mensaje M1 y verifica su coincidencia con el recibido. Si coincide es que quien calculó el VRM2 recibido es la Parte B pues únicamente ella conoce el valor VAM2. Así queda autenticada la Parte B como emisora del mensaje M2 y también la integridad del mensaje recibido y que el M2 es la respuesta al M1 enviado ya que en él se ha usado el valor VAM2. De ésta forma, la Parte A sabe que ciertamente está dialogando con la Parte B, completándose el proceso de autenticación mutua.

d) Con el fin de que la Parte B sepa con seguridad que el M2 llegó a la Parte A y que, por lo tanto, el proceso de autenticación mutua ha sido realizado correctamente, será necesario que la Parte A envíe a la Parte B un M3 confirmando la recepción del M2, sabiendo la Parte B que, siguiendo el procedimiento objeto de la invención, la Parte A responderá únicamente si ha recibido el mensaje M2 y comprobado que para obtener su valor resumen VRM2 se usó el VAM2 enviado en el M1. Siendo así:

- Compone el mensaje IdB, IdA, TS3, DATOS, VAM3, con el TS3 del momento y los DATOS a enviar, y calcula su función resumen VRM3.
- Envía a la Parte B (IdB) un mensaje M3 conteniendo, entre otros posibles valores, los de: IdB; IdA; TS3, DATOS, VRM3.

De esta forma cuando la Parte B reciba el mensaje verificará que el VRM3 recibido coincide con el calculado usando los valores recibidos junto con el VAM3 que recibió en el M1 y, si coinciden el VRM3 recibido con el calculado, la Parte B tendrá la seguridad de que es la Parte A su emisor pues únicamente ella conoce el VAM3 y también sabe que el mensaje M2 ciertamente fue recibido por la Parte A y ésta es su respuesta, ya que, siguiendo el procedimiento de autenticación objeto de la invención, la Parte A no hubiera enviado éste mensaje si no hubiera recibido previamente el M2 correcto. También queda asegurada la integridad del mensaje M3 recibido.

Así, el procedimiento de autenticación mutua queda completado desde el punto de vista de quienes han sido los creadores de los mensajes intercambiados en el diálogo, Parte A y Parte B, y con la seguridad de la autenticidad de los datos y su integridad. Y queda autenticado,

acreditado, que la información enviada por la Parte A en el mensaje M1 sí que le llegó a la Parte B y que la recibida en el M2 es justamente su respuesta al M1, así como que el M2 le llegó a la Parte A y que el M3 es la respuesta al M2; con lo que ya ninguna de las dos Partes puede alegar el desconocimiento o repudio de la operación.

En el caso en que la operativa a autenticar requiera que la Parte A sepa que su M3 ciertamente llegó a la Parte B será necesario que la Parte B envíe a la Parte A un nuevo mensaje M4 y para ello, en éste caso, se habrá generado y transmitido al inicio otro valor pseudoaleatorio VAM4. Y así sucesivamente.

La misma forma de proceder permitirá llevar a cabo un diálogo iniciado por la Parte B que tiene como destinatario la Parte A.

En todos los mensajes, de manera opcional, por su interés para su posterior auditoría y gestión, también podrá viajar cifrado un valor que agrupe y diferencie todos los mensajes que pertenecen a un mismo diálogo.

En todos los mensajes, de manera opcional, por su interés para la operativa y controles, también podrá viajar cifrado el identificador del emisor del mensaje en la red de comunicación que soporta el diálogo.

- Por su importancia en cuanto a eliminar el riesgo que pueda suponer el uso de una misma clave fija CCAB para el cifrado y descifrado del primer mensaje M1 que se intercambian las partes intervinientes en el diálogo autenticado, a continuación se detalla una forma de llevar a cabo el diálogo que consigue el que el valor de la clave, usada para el cifrado y descifrado del mensaje M1, sea diferente para un diálogo que se lleve a cabo después de otro en el que las partes A y B se hayan intercambiado correctamente los mensajes cifrados M1 y M2.
Así, la clave fija CC pasa a ser una clave de un único uso, clave tipo OTP (One Time Password), y ya entonces todas las claves de cifrado que usa el sistema son claves de un único uso. La principal ventaja es que haciendo uso de claves OTP se impiden los ataques de REPLAY, también llamado ataque de reproducción o de reinyección, que es un ciberataque en el cual una entidad intercepta y a continuación repite una transmisión de datos con malas intenciones. Otra ventaja es la de que hace al sistema más resistente frente ataques de fuerza bruta, ya que cada vez que cambia la clave, los intentos realizados anteriormente para romper la clave de cifrado anterior son inútiles y hay que empezar de nuevo.

Para ello:

- en el momento de integrarse una nueva Parte en el sistema de autenticación dicha Parte compartirá un valor inicial de la clave de cifrado CC con cada una de las otras Partes con las que quiera poder intercambiar mensajes, siendo diferente para cada pareja de partes;

- la Aplicación de Autenticación de la Parte B para verificar que el mensaje M1 viene de la Parte A descifra el mensaje con el valor CCAB y si con éste valor no se puede verificar su autenticidad, y el anterior diálogo terminó sin que la Parte A recibiera el M2, lo descifra con el valor usado para el último mensaje tratado y verificado que estará guardado en una variable CCUUAB;
- la Aplicación de Autenticación de la Parte B, después de comprobar que el M1 recibido viene de la Parte A:
    - se guarda el valor usado en el cifrado y descifrado de dicho M1 en una variable CCUUAB;
    - genera un nuevo valor para la clave de cifrado CCAB a usar en el próximo M1 que reciba de Parte A;
    - comunica a la Parte A el nuevo valor de CCAB por medio del mensaje cifrado M2.

- la Aplicación de la Parte A, después de comprobar que el mensaje M2 recibido viene de la Parte B, guarda en CCAB el valor de la nueva clave de cifrado recibido en el M2 para ser usada en el próximo M1 a enviar a la Parte B.

Operando de esta forma el valor de la CCAB será diferente cada vez que las Partes se intercambien correctamente los mensajes M1 y M2.

A continuación se describen algunas características diferenciadoras de la implementación del sistema:

- Las Partes que se intercambian mensajes en un diálogo comparten una clave de cifrado que únicamente se emplea para el cifrado y descifrado del primer mensaje que se intercambian de forma que se facilita su ocultación al minimizar su tiempo de uso y de posible exposición. Existen otros sistemas que aplican la misma clave de cifrado en todos los mensajes que se intercambian en su diálogo con lo que se aumenta considerablemente el tiempo de su posible exposición y aumenta el riesgo de que dicha clave pueda llegar a ser conocida por un intruso.

- El sistema de cifrado y autenticación de los mensajes aplica un protocolo y un algoritmo de cifrado que, haciendo uso de una clave fija y valores pseudoaleatorios, cifra y autentica los mensajes que se envían y reciben las Partes integradas en el Sistema, que implementa dicho Sistema, de manera que se llega a conseguir una autenticación mutua de las Partes. Existe algún sistema de cifrado y autenticación en los que el valor aleatorio, a emplear en el cifrado de los mensajes del diálogo que se va a iniciar, se envía al Destinatario cifrado con una clave fija compartida pero el mensaje en que se envía no queda validado por un proceso de autenticación mutua con los problemas que se pueden derivar de ello pues no queda verificada la llegada del mensaje a su verdadero destinatario y tampoco la autenticidad del emisor.

- El sistema de cifrado y autenticación de los mensajes que se usa en el sistema de autenticación utiliza un algoritmo de cifrado avanzado (tipo AES 128 o 256), de forma que si alguien realizara un ataque de fuerza bruta para intentar romper el cifrado, con la tecnología actual, las estimaciones de tiempo y recursos requeridos lo hacen no asumible y no rentable.

- El hecho de que la secuencia de los mensajes que se intercambian en el procedimiento venga fijada por la presencia en el mensaje de los valores pseudoaleatorios VAMx, y no por un valor fijo predeterminado que establezca un orden en la secuencia de los mensajes, fortalece la seguridad del cifrado ya que la mayoría de las técnicas usadas para romper los cifrados lo que hacen es buscar la existencia de valores fijos presentes en el texto cifrado.

- El sistema de cifrado y autenticación de los mensajes, que se usa en el sistema de autenticación, sólo necesita de una clave de cifrado, CC que está disponible en las aplicaciones de autenticación de los intervinientes, junto con valores pseudoaleatorios que se generan en el momento. Comparando ésta forma de proceder con la de otros posibles sistemas de autenticación que utilizan claves OTP almacenadas para el cifrado de sus mensajes, es evidente que se evita la necesaria disponibilidad de recursos de almacenamiento y se simplifica enormemente el funcionamiento del sistema y su mantenimiento en cuanto que se eliminan los procesos de recarga de claves ya usadas y la sincronización puntual necesaria en éste tipo de sistemas.

- La implementación del sistema se puede hacer de forma que el valor de la clave CC y/o la generación del valor pseudoaleatorio y/o su cifrado se lleven a cabo en un dispositivo externo

que únicamente se conecta a la Aplicación con el fin de proporcionar estos valores. Si alguien copia la Aplicación dicha copia no dispone de dicho dispositivo y no podrá funcionar.

- En la implementación del procedimiento de autenticación, el sistema de autenticación puede usar un tercer factor de autenticación (3FA) del usuario/parte fundamentado en el uso de un Elemento que almacena un valor que complementa el valor de autenticación y que debe ser aportado por el usuario/parte para que la autenticación mutua finalice correctamente. En éste caso si copian o roban el dispositivo de autenticación, junto con su aplicación de autenticación, no podrán realizar ninguna operación de autenticación ya que les faltaría dicho Elemento.

- Cuando, en la implementación del sistema de autenticación en la Aplicación, es necesaria la intervención del usuario dicha intervención se minimiza limitándola a activar la aplicación de autenticación – normalmente con su huella dactilar o aproximando (con sistema NFC (*Near-field communication* o campo de comunicación cercano)) una tarjeta al dispositivo, escaneando un QR, conectando un microcontrolador, etc - y a, con un clic, autorizar o rechazar la operación. Con ello se evitan las molestias y errores de cualquier otro tipo de intervención que en la mayor parte de los sistemas de autenticación existentes obligan a la memorización de un PIN y al engorroso tecleo de datos en su dispositivo, lo que es origen de muchos errores, pérdida de tiempo y gastos.

- El sistema de autenticación identifica al Usuario (Parte) y lo autentica a él, y a los mensajes que se intercambian, frente al otro interviniente en el diálogo y para su funcionamiento, normalmente, requiere del usuario 2 Factores de Autenticación (2FA), el código de activación y la Aplicación instalada en su dispositivo.

- El sistema de autenticación, implementado y ejecutado bajo ciertas condiciones, que garanticen que únicamente la aplicación de autenticación pueda acceder al valor CC, facilita la autenticación de mensajes entre dispositivos llevada a cabo de forma automática, sin intervención manual, por lo que el campo de aplicación del sistema se amplía a cualquier dispositivo que requiera enviar un mensaje autenticado y cifrado a otro dispositivo previamente emparejado con él por medio del sistema de autenticación.

- La autenticación mutua de las partes, que se aplica en la implementación del procedimiento de autenticación, permite realizar operaciones sin miedo a que se esté produciendo un problema de *Phishing o Pharming* ya que no da por terminada correctamente una operación

si antes no se han identificado mutuamente los intervinientes.

- El hecho de que en el sistema de autenticación los mensajes que se intercambian, M2 y sucesivos, viajen cifrados y/o autenticados por una clave aleatoria de un solo uso equivale a que los mensajes estén viajando cada vez por un canal de comunicación lógico diferente con lo que esto supone en cuanto a evitar posibles ataques del tipo *Man In The Middle.*

- En la implementación del sistema de autenticación se puede hacer que desde una aplicación AA1 de una Parte A (ejecutada en un Servidor Seguro o que hace uso de una autenticación 2FA para su activación) se pueda enviar de forma segura una Solicitud Autenticada que pide la ejecución de una Operación a cualquiera de las Aplicaciones Operativas (AO) con las que se relaciona la aplicación AA2, de la Parte B, dentro del Sistema Informático que soporta dicha AA2.

- En la implementación del sistema de autenticación, la autenticación mutua de las partes junto con la autenticación de los mensajes intercambiados permite confirmar, firmar y evitar el repudio de cualquier tipo de operación realizada entre las Partes. Por ejemplo, una solicitud de transferencia en una Entidad Financiera o la ejecución de un comando dentro de un Sistema de Control de Procesos en la Industria o en el Internet de las Cosas.

- Cualquiera de las características diferenciadoras citadas anteriormente aplicables al caso en que la clave de cifrado que se usa para cifrar y descifrar el mensaje M1, que se intercambian las Partes que dialogan, es diferente para cada nuevo diálogo terminado correctamente. Esta característica del sistema aporta una mejora importante en cuanto a que el tiempo de validez de una misma clave de cifrado CC, almacenada en las Aplicaciones de Autenticación, se reduce al tiempo que pase entre dos diálogos mantenidos por las partes. Así, la clave fija CC pasa a ser una clave de un único uso (clave tipo OTP) con lo que se evitan ataques de Replay y se mejora la resistencia ante los ataques de fuerza bruta empleados para hacerse con la clave de cifrado.

A continuación, se describen algunos ejemplos de casos de aplicación del sistema.

- Sistema para la autenticación mutua multifactor de las Partes que quieren llevar a cabo un Diálogo Seguro entre ellas con un intercambio de mensajes cifrados y autenticados y que pueden quedar a su exclusiva disposición cifrados con un segundo valor únicamente conocido

por ellos.

- Sistema para la autenticación de las Partes que intervienen en la solicitud de una operación y su posterior autorización para que sea ejecutada, evitando su repudio. Como ejemplos, la operación puede ser desde una solicitud de acceso a un Portal web hasta la autenticación y confirmación de una operación solicitada en un Portal web o la autorización y confirmación de una operación solicitada por medio de un dispositivo que opere con tarjetas de identificación y/o pago.

- Sistema de Intercambio de Mensajes Cifrados y Autenticados entre Partes usuarias del Sistema que las permite enviar/recibir mensajes cifrados y autenticados a/de cualquier otra Parte usuaria del Sistema haciendo uso de un Tercero de Confianza con el que se comunican las dos Partes interesadas en el Intercambio de Mensajes.

- Sistema en el que las Partes A y B son dos Servidores, integrados en una red de comunicación, en la que la Aplicación de Comunicación de la Parte A puede recibir mensajes de la Aplicación de Comunicación de la Parte B, y viceversa, donde dichos mensajes se caracterizarán por estar cifrados y autenticados facilitando la creación de una Red Segura de Comunicaciones.

- Sistema válido para la autenticación de los mensajes que se puedan intercambiar los Controladores de Sensores con su Sistema de Control de Procesos Industriales y éste con los Usuarios Responsables de su regulación por medio de la autenticación de los comandos enviados por el usuario al sistema para su ejecución. De forma similar será aplicable a los mensajes que se intercambian los Sensores con sus Controladores. Todo ello también aplicable al ámbito de los Sistemas de Internet de las Cosas (IoT).

Finalmente, cabe mencionar que, en el procedimiento de autenticación de la invención, se entiende por Parte un Ente, persona o máquina física o lógica, que dialoga con otro Ente por su mutuo interés en conseguir resolver una misma operación con el fin de obtener un resultado concreto en el ámbito de su actividad. Estos Entes deberán tener la capacidad de llevar a cabo las actividades a desempeñar por las Partes en el procedimiento descrito, o actividades equivalentes, siempre que tengan los mismos efectos.

En resumen, el sistema de autenticación objeto de la invención contempla varias formas de llevar la autenticación mutua de los comunicantes, entre ellas:

i / - Sistema con diálogo iniciado automáticamente entre AAA y AAB:
Se lleva a cabo, siguiendo el sistema de cifrado y autenticación objeto de la invención, por medio de un diálogo, que se inicia automáticamente entre las dos aplicaciones de autenticación AAA y AAB cuando a la AAA le llega un evento predeterminado (ejemplo: le llegan DATOS a enviar a la AAB). Las Aplicaciones de Autenticación están previamente activas y disponen de la clave de cifrado CCAB que comparten.

ii / - Sistema con diálogo iniciado por una Parte A (persona física) disponiendo de dos factores de autenticación, la AAA y el CA:

Se lleva a cabo siguiendo el sistema de cifrado y autenticación objeto de la invención mediante un diálogo entre las dos aplicaciones de autenticación AAA y AAB que lo inicia la Parte A (persona física) activando la aplicación AAA con su código de activación CA. La AAB está ya activa y dispone de la CCAB que comparte con AAA.

iii / - Sistema con diálogo iniciado por una Parte A (persona) disponiendo de tres factores de autenticación, la AAA, el CA y el 3FA:

Se lleva a cabo siguiendo el sistema de cifrado y autenticación objeto de la invención mediante un diálogo entre las dos aplicaciones de autenticación AAA y AAB que lo inicia la Parte A (persona física) activando la aplicación AAA con su código de activación CA. La Parte A deberá aportar a la AAA el tercer factor de autenticación 3FA para que la AAA pueda validar el mensaje M2 enviado por la AAB. La AAB está ya activa y dispone de la CCAB que comparte con AAA.

iv / - Sistema simplificado con diálogo iniciado automáticamente entre AAA y AAB: igual al caso i pero aplicando el sistema simplificado de cifrado y autenticación.

v / - Sistema simplificado con diálogo iniciado por Parte A (persona) disponiendo de dos factores de autenticación, la AAA y el CA: Igual al caso ii pero aplicando el sistema simplificado de cifrado y autenticación.

vi / - Sistema simplificado con diálogo iniciado por Parte A (persona) disponiendo de tres factores de autenticación, la AAA, el CA y el 3FA: Igual al caso iii pero aplicando el sistema simplificado de cifrado y autenticación.

vii / - Sistema con claves de un único uso con Diálogo Automático fijando la CCAB para el siguiente Diálogo:
Igual al caso i pero aplicando el sistema de cifrado y autenticación con claves de un único uso donde la clave de cifrado CCAB que se usa en un diálogo ha sido creada en el anterior diálogo en el que las partes se han intercambiado los mensajes M1 y M2.

viii / - Sistema con claves de un único uso con Diálogo iniciado por Parte A (persona) disponiendo de dos factores de autenticación, la AAA y el CA:
Igual al caso ii pero aplicando el sistema de cifrado y autenticación con claves de un único uso.

ix / - Sistema con claves de un único uso con Diálogo iniciado por Parte A (persona) disponiendo de tres factores de autenticación, la AAA, el CA y el 3FA:
Igual al caso iii pero aplicando el sistema de cifrado y autenticación con claves de un único uso.

Relación de acrónimos utilizados:

Aplicación de Autenticación (AA)
Aplicación de Autenticación parte A (AAA)
Aplicación de Autenticación parte B (AAB)
Identificador (Id)
Clave de Cifrado (CC)
Código de Activación (CA)
Mensaje (M)
Timestamp del momento (TS)
Valores de Autenticación (VA)
Valor Resumen (VR)
Factor de Autenticación, (FA)

DESCRIPCIÓN DE LOS DIBUJOS

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, se acompaña a la presente memoria descriptiva, como parte integrante de la misma, de un juego de planos en que con carácter ilustrativo y no limitativo se ha representado lo siguiente:

La figura número 1.- Muestra una representación esquemática de los principales elementos que intervienen en el sistema de autenticación objeto de la invención y la relación de cómo interacciona el sistema de autenticación con el sistema informático de la empresa que gestiona las aplicaciones operativas para llevarlo a cabo.

La figura número 2.- Muestra un diagrama de los pasos que comprende el esquema operativo y flujo mensajes sistema de autenticación cuando los datos de la operación realizada por la Parte A desde un dispositivo D1A son captados por la AA1 de forma automática (con un QR, vía NFC, o cualquier otro medio de comunicación posible) procedentes del D1A.

La figura número 3.- Muestra un diagrama de los pasos que comprende el esquema operativo y flujo de mensajes del sistema de autenticación cuando AA1 inicia la autenticación de una operación que la Parte A solicitó a una Aplicación Operativa AO desde su dispositivo D1A.

La figura número 4.- Muestra un diagrama de los pasos que comprende el esquema operativo y flujo de mensajes sistema de autenticación para una autenticación mutua entre dos Partes que autentica un mensaje enviado por la Parte A a la Parte B y la Parte B confirma su recepción.

La figura número 5.- Muestra un diagrama de los pasos que comprende el flujo de mensajes sistema de autenticación para una autenticación mutua confirmada entre dos Partes.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

A la vista de las mencionadas figuras, y de acuerdo con la numeración adoptada, se puede observar en ellas una representación y diversos esquemas de realización no limitativa del sistema de la invención y que, por tanto, no excluyen cualquier otro que pueda darse, de características similares en el que se intercambien AA1 y AA2 mensajes según el sistema de

autenticación descrito, que permita completar su autenticación mutua y una posible confirmación de una operación realizada entre ellos.

Cabe mencionar que, para simplificar la explicación de los esquemas de las figuras, además de los acrónimos ya señalados en anteriores párrafos, en adelante se van a utilizar las siguientes abreviaturas:

D1A Dispositivo operativo desde el que está operando un usuario

DO Datos de la Operación

AA1 Aplicación de Autenticación de la Primera Parte

AA2 Aplicación de Autenticación de la Segunda Parte

AO Aplicación de la parte B que soporta la Operativa que está realizando el usuario o parte A.

Así, en la figura 1 se ha representado, esquemáticamente, una representación de los principales elementos que comprende el sistema de autenticación (1) con que se lleva a cabo el procedimiento objeto de la invención, donde por una parte, referenciado como (2), se muestran los dispositivos y herramientas informáticas que utilizan los usuarios demandantes de operaciones o parte A, concretamente, al menos un D1A y AO, así como un D2A y AA1, y por otra parte, referenciado como (3), se muestran las herramientas del sistema informático de la empresa, parte B, es decir, D1B y AA2 y las aplicaciones operativas AP1, AP2, AP3.

Atendiendo a la figura 2, se observa cómo el esquema operativo y flujo mensajes del sistema de autenticación, cuando los datos de la operación solicitada por la Parte A desde un dispositivo D1A son captados por la AA1 de forma automática (con un QR, vía NFC, o cualquier otro medio de comunicación posible) procedentes del D1A, comprende los siguientes pasos:

a) EL D1A proporciona a la AO los DO a autenticar y confirmar. Y la AO prepara los DO para ser enviados al D1A y AA2.

b) La AO envía a D1A los DO en el formato adecuado para poder ser captados por AA1.

c) La AO envía a AA2 los DO. La AA2 guarda los DO a la espera de su autenticación

d) La AA1 capta del D1A los DO. La AA1 presenta al usuario los DO y espera su confirmación. Si los confirma crea, según el procedimiento de autenticación simplificado, el mensaje M1 y lo envía a AA2.

e) La AA2 descifra, según el procedimiento de autenticación simplificado, el M1 y verifica los DO con los que tiene en espera. Si son correctos, crea, según el procedimiento de

autenticación simplificado, y envía a AA1 el mensaje M2.

f) La AA2 comunica a la AO el resultado.

g) La AA1 procesa el M2 según el procedimiento de autenticación simplificado, y presenta los datos al Usuario, confirmando que la autenticación se ha realizado correctamente.

h) La AO comunica el resultado al D1A.

Atendiendo a la figura 3, se aprecia el esquema operativo y flujo de mensajes del sistema de autenticación, cuando AA1 inicia la autenticación de una operación que la Parte A solicitó a una Aplicación Operativa AO desde su dispositivo D1A, comprende los siguientes pasos:

a') El D1A proporciona a la AO los DO a autenticar y confirmar. La AO prepara los DO y los envía a AA2.

b') La AA2 guarda los DO, a la espera de que llegue de la AA1 la petición de autenticación.

c') La AA1 envía un mensaje cifrado M1 a la AA2 para iniciar la autenticación de una operación que ha sido solicitada por el usuario desde el D1A.

d') La AA2 verifica que viene de AA1 y que para dicho usuario hay una operación en espera de autenticación. Crea el mensaje M2 con los DO y se lo envía a AA1.

e') La AA1 descifra el M2, verifica que viene de AA2 y se los presenta al usuario para su autorización. Crea el mensaje M3 con los DO y el resultado de la autorización y lo envía a AA2.

f') La AA2 descifra el M3, verifica que viene de AA1, controla que coinciden los DO que tiene con los DO recibidos y comunica el resultado a la AO y crea un mensaje M4 que envía a AA1 para comunicar el resultado.

g') La AA1 trata el M4 y presenta al usuario el resultado de la operación.

h') La AA2 comunica a la AO el resultado.

i') La AO comunica el resultado al D1A.

Atendiendo a la figura 4, se aprecia que el esquema operativo y flujo de mensajes del sistema de autenticación para una autenticación mutua entre dos Partes que autentica un mensaje enviado por la Parte A a la Parte B y la Parte B confirma su recepción comprende:

a'') La AA1 envía un mensaje cifrado M1 a la AA2 e inicia la operación de autenticación mutua.

b'') La AA2 verifica, con el procedimiento de descifrado, que el M1 viene de de AA1 con lo que AA1 queda autenticado frente a AA2 como emisor del mensaje y también el contenido del mensaje. AA2 crea el mensaje M2 y lo envía a AA1 para terminar el proceso de autenticación

mutua y confirmar que le llegó el M1.

c'') La AA1 descifra el M2 y comprueba que es la respuesta que proporciona AA2 al mensaje M1 con la que AA2 ya queda autenticado frente a AA1 y se cierra el proceso de autenticación mutua para el diálogo realizado. AA1 también sabe que a AA2 le llegó el M1.

Y, atendiendo a la figura 5 que aprecia que los pasos que comprende el flujo de mensajes del sistema de autenticación para una autenticación mutua confirmada entre dos Partes son:

a''')La AA1 envía un mensaje cifrado M1 a la AA2 e inicia la operación de autenticación mutua.

b''') La AA2 verifica, según el procedimiento, que el M1 viene de AA1 con lo que AA1 queda autenticado frente a AA2 como emisor del mensaje. AA2 crea el mensaje M2 y lo envía a AA1 para terminar el proceso de autenticación mutua y confirmar que llegó el M1.

c''') La AA1 trata del M2 y comprueba que es la respuesta que proporciona AA2 al mensaje M1 con lo que AA2 ya queda autenticado frente a AA1 y se cierra el proceso de autenticación mutua para el diálogo realizado. AA1 también sabe que a AA2 le llegó el M1. Para que la Parte B sepa que la autenticación mutua ha terminado correctamente, la Parte A le envía un mensaje M3

d''') La AA2 verifica, según el procedimiento, que el M3 viene de AA1 y así sabe que terminó correctamente el proceso de autenticación mutua y que le llegó el M2 a AA1.

A continuación, se describen diferentes ejemplos de modo de uso del sistema de autenticación, según la invención.

Así, como primer ejemplo de Modo de uso del sistema de autenticación y cifrado, objeto de la invención, veremos cómo se aplica al caso en que un usuario del sistema de autenticación, Parte A, quiere transmitir un mensaje cifrado a otro usuario del sistema de autenticación, Parte B, asegurándose de que dicho mensaje ciertamente ha llegado al usuario destinatario.

Características:

Parte A y Parte B:

- están inequívocamente identificados, por sus IdA e IbB, dentro del sistema de autenticación de mensajes soportado por la red de comunicaciones que les permite intercambiar dichos mensajes, estando comunicadas las partes por uno o más canales de comunicación que les

permiten intercambiar dichos mensajes;
- disponen de su Aplicación de Autenticación, con todos sus componentes, en un dispositivo que garantiza que: la clave de cifrado CC solo puede ser conocida y usada por él; y que las operaciones de cifrado y descifrado también se realizan de forma segura. Para ello puede hacerse uso de medios del tipo Hardware Security Module (HSM).

Para los diálogos entre A y B necesitan, en sus aplicaciones de autenticación:

- que las partes activen sus aplicaciones de autenticación aportando sus códigos de activación con el medio establecido;
- compartir el valor CC;
- un generador de Valores Pseudoaleatorios, que serán usados en los mensajes Mx;
- un algoritmo de cifrado, que comparte con el resto de las Partes del Sistema, que les permite cifrar y descifrar los mensajes que se envían/reciben.

Operativa:

Parte A
Inicia el procedimiento para un diálogo con la Parte B, en el que se van a intercambiar dos mensajes, y para ello, haciendo uso de su Dispositivo y su Aplicación de Autenticación AAA:

- Genera y guarda dos Valores Pseudoaleatorios, CCM2, VAM2 a usar como Clave de Cifrado y Valor de Autenticación en el mensaje M2. Estos valores generados tendrán un tiempo de validez determinado que será controlado en su proceso de uso;
- Obtiene el Timestamp del momento TS; prepara la información a enviar conteniendo, al menos, los valores IdB, IdA, TS, CCM2, VAM2, y DATOS, donde DATOS contendrá la información que se desee comunicar a la Parte B; aplica a ésta información una función resumen (función hash tipo Secure Hash Algorithm o cualquier otro algoritmo similar) obteniendo un Valor Resumen de la información a transmitir en el mensaje M1, VRM1; cifra con CC, obteniendo CC(TS, CCM2, VAM2, DATOS, VRM1).
- Envía a la Parte B un mensaje M1 conteniendo, entre otros posibles, los datos: IdB; IdA; CC(TS, CCM2, VAM2, DATOS, VRM1).

Opcionalmente, por su interés para la operativa y controles, también podrá viajar cifrado por CC el identificador del emisor del mensaje en la red de comunicación que soporta el diálogo.

Parte B

Continúa con el procedimiento para un diálogo con la Parte A, y para ello, haciendo uso de su Dispositivo y su Aplicación de Autenticación AAB:

- Recibe el mensaje M1 y continúa con el procedimiento de autenticación del diálogo iniciado. Para ello:

  - Verifica el Identificador de Parte A.
  - Descifra, con CC que comparte con la parte A, el CC (TS, CCM2, VAM2, DATOS, VRM1); aplicando la misma función resumen a los mismos valores recibidos obtiene el Valor Resumen que debe tener el VRM1 recibido y si coincide el calculado con el recibido es que el descifrado ha sido realizado correctamente. Esto quiere decir que el valor CC es el que se usó para cifrar y por lo tanto el que creó el mensaje y realizó el cifrado ha sido la Parte A, ya que sólo ella conoce dicho valor. Además queda garantizada la integridad y confidencialidad de la información recibida. También, opcionalmente, se controlará que el Timestamp TS recibido es igual o mayor que el del último mensaje tratado y que está dentro de un rango de valores convenido.

- La Parte B, una vez recibido el M1 y verificado que viene de la Parte A, prepara y envía, a la Parte A, un mensaje M2 para comunicar a la Parte A que ha recibido el M1. Para ello:

  - Compone el mensaje (TS2, VAM2, DATOS), con el TS2 del momento y los DATOS de confirmación a enviar, y lo cifra con CCM2.
  - Envía a la Parte A (IdA) un mensaje M2 conteniendo, entre otros posibles valores, los de: IdA; IdB; CCM2(TS2, VAM2, DATOS).

Parte A

Recibe de Parte B el mensaje M2 : IdA; IdB; CCM2(TS2, VAM2 DATOS) y continúa con el procedimiento de autenticación del diálogo ya iniciado. Para ello:

- Verifica el Identificador de Parte B.
- Descifra, con CCM2 enviado a la parte B en el mensaje M1, la información del M2 para obtener el VAM2 y verificar su coincidencia con el enviado en el M1 con lo que se asegura de que el descifrado ha sido correcto y que el M2 es la respuesta al M1 enviado ya que contiene el valor VAM2, con lo que queda autenticado el mensaje. Como únicamente es la Parte B la

que conoce el valor CCM2 con el que llegó cifrado el mensaje M2, queda asegurada la autenticidad de la Parte B como creador del mensaje M2 y, de ésta forma, la Parte A sabe que ciertamente está dialogando con la Parte B, completándose el proceso de autenticación mutua y la confirmación de que el mensaje M1 fue recibido por la Parte B y posteriormente no podrá alegar su desconocimiento. Al viajar el mensaje cifrado también queda garantizada su integridad y confidencialidad.

Operando de esta forma las Partes se han transmitido una información cifrada, que únicamente conocerán ellas, asegurándose el emisor que ha llegado al destinatario correcto (sólo la Parte B puede haber generado el M2 recibido) y asegurándose el destinatario quién ha sido el verdadero emisor (sólo la Parte A puede haber generado el M1 recibido).

Un esquema de esta operativa y flujo de mensajes queda representado en la Figura 4.

Una aplicación real del caso expuesto sería aquel en que un servidor de correo electrónico de una parte A envía un mensaje certificado con acuse de recibo a otro servidor de correo electrónico de una parte B. Operando de esta forma la parte A se asegura de que la información del correo le ha llegado a la parte B y únicamente a ella, y, a su vez, la parte B está segura de que la información procede de la parte A. Así se puede evitar recibir correos cuyo emisor real está suplantando la identidad de una parte y se aprovecha para transmitir una información falsa con objeto de cometer un fraude. Un ejemplo de este tipo de fraude es el *Business Email Compromise* (BEC) o estafas *MAN-IN-THE-EMAIL*.

Como segundo ejemplo de Modo de uso del sistema de autenticación y cifrado, objeto de la invención, a continuación se aplica a la ejecución de una operación solicitada por la Parte A a la Parte B, operación en la que es necesaria la autenticación mutua de las Partes y la confirmación de la solicitud por la Parte solicitante antes de la ejecución de dicha operación. Como peculiaridad de la operativa se tiene el hecho de que los datos de la operación a ejecutar los recibe la aplicación de autenticación AA1 por medio de una comunicación entre los dispositivos D1A y D2A (que soporta la AA1) de la Parte A.

Características

La realización hace uso del procedimiento de autenticación simplificado descrito. Por ello, únicamente la Parte Central (Parte B) puede dialogar con todas las otras Partes (Parte A),

integradas en el sistema de autenticación que soporta el procedimiento de autenticación, mientras que éstas únicamente pueden dialogar con la Parte Central.

El procedimiento de autenticación sólo funcionará correctamente en una aplicación de autenticación AA específica de una Parte A y con un código de activación CA determinado. Así, aunque alguien copie la AA se encuentra con el problema de desconocer el CA.

Si a la Parte Central la llamamos Parte B y al resto de Partes las llamamos genéricamente Parte A, las características a destacar en éste diálogo autenticado según el sistema de autenticación son:

- las partes, Parte A y Parte B, están inequívocamente identificadas entre ellas, dentro del sistema de autenticación, mediante un primer y segundo identificador;
- la Parte A dispone de, al menos, un primer dispositivo, físico o lógico, (D1A) y un segundo dispositivo, físico o lógico, (D2A) en el que reside una primera aplicación de autenticación (AA1);
- el primer dispositivo de la primera parte D1A con gran frecuencia es un PC, (aunque también puede ser un teléfono móvil, cajero automático, Terminal Punto de Venta físico o lógico, o cualquier otro dispositivo, físico o lógico, con capacidades equivalentes), que pueda solicitar operaciones a un sistema informático y colaborar en su realización en representación de la Parte A.
- el segundo dispositivo de la primera parte D2A normalmente será un teléfono móvil inteligente aunque también puede ser cualquier otro dispositivo, físico o lógico, con capacidades equivalentes, en el que pueda ejecutarse el software de la aplicación de autenticación AA1;
- para activar dicha primera aplicación de autenticación AA1 la Parte A tendrá que teclear un Código de Activación CA o hacer uso de un medio (huella dactilar de la Parte A, una Tarjeta de Acceso tipo NFC o con un código QR, un microcontrolador, o cualquier otro medio similar) el cual aportará a la AA1 el Código de Activación CA;
- la Parte B dispone de un dispositivo, físico o lógico, (D1B) en el que reside una segunda aplicación de autenticación (AA2), relacionada inequívocamente, dentro del sistema de autenticación, con dicha primera aplicación de autenticación AA1. Esta AA2 está activa y se ejecuta en un entorno seguro con las medidas de seguridad necesarias para poder pensar que sólo la Parte B puede tener acceso a la aplicación AA2 y a sus datos;
- dicha AA2 forma parte del sistema informático de la Parte B y puede interaccionar con

las aplicaciones operativas (AO) soportadas por dicho sistema informático, con las que la Parte A, desde su primer dispositivo (D1A), puede realizar operaciones relativas a la actividad operativa del sistema informático de la Parte B. Una representación ilustrativa se puede ver en la figura 1;

- dicha AA2 puede relacionarse con tantas aplicaciones de autenticación de Partes A como usuarios tenga el sistema informático de la Parte B;
- dichas primera y segunda aplicación, AA1 y AA2, disponen cada una de ellas de un identificador único dentro del sistema de autenticación, IdA e IdB respectivamente;
- dichas primera y segunda aplicación comparten una misma clave de cifrado CC que usarán a lo largo del procedimiento de autenticación mutua;;
- dicha primera aplicación AA1 dispone de un algoritmo generador de valores pseudoaleatorios;
- dichas primera y segunda aplicación, AA1 y AA2, disponen cada una de ellas del mismo algoritmo de cifrado AES 128, o cualquier otro de características similares, para sus operaciones de cifrado/descifrado;
- la AA2 tendrá tantos diferentes valores de clave de Cifrado CC como aplicaciones de autenticación de Partes A estén relacionadas con ella;
- los dispositivos de dichas Parte A y Parte B están en comunicación por medio de uno o más canales de comunicación, físicos o lógicos, diferentes;
- opcionalmente, todos los mensajes que se intercambian las Partes A y B son guardados por el sistema de autenticación en un fichero para su posterior uso como fichero de registro de la actividad del sistema (LOG).

Operativa

- la Parte A por medio de su primer dispositivo D1A solicita la ejecución de una operación a una de las aplicaciones operativas (AO) de la Parte B;
- la aplicación operativa AO recibe del dispositivo de la Parte A, D1A, la solicitud de operación con los datos de la operación DO. Esta solicitud con sus datos DO deberán ser autenticados y autorizados por la Parte A desde su Aplicación de Autenticación debido a la falta de seguridad del canal por el que se ha recibido la solicitud y a la necesidad de autenticación/confirmación que requiere la ejecución de la operación;
- la aplicación operativa AO prepara los datos de la operación DO recibidos y los envía a la aplicación de autenticación de la Parte B, AA2, la cual los recibe y deja a la espera de que sean autenticados por la Parte A;

- la aplicación AO toma los datos de la operación DO recibidos y los formatea adaptándolos al medio en que posteriormente van a ser leídos por la AA1 desde el D1A (leyendo un QR, transmitiéndose vía NFC,…) y se los reenvía al dispositivo D1A.

- opcionalmente, puede ser la misma AA2 la que se encargue de éste formateo de los datos que a través de la AO los envía al D1A.

- la Parte A activa su aplicación de autenticación AA1 aportando el código de activación CA;
- la Parte A haciendo uso de una comunicación posible entre D1A y D2A (por ejemplo, escaneando con su AA1, soportada por el D2A, un código QR que la AO presenta en su página web en el D1A, o comunicándose vía NFC la AA1 con el D1A, o cualquier otra forma de comunicación posible entre la AA1 y el D1A) , recibe en su AA1 los datos DO de la operación a autenticar, y confirmar, y los presenta en pantalla al usuario (Parte A) para que los confirme como datos de la operación a realizar. Si la Parte A confirma los datos será su aplicación de autenticación AA1 la que envía a la aplicación de autenticación de la Parte B un primer mensaje cifrado M1, según el procedimiento de autenticación simplificado, en el que ya viajan cifrados los datos de la operación, solicitada y confirmada por la Parte A, que la Parte B tiene pendiente de autenticar;
- la aplicación de autenticación de la Parte B, AA2, recibe dicho primer mensaje M1 cifrado según el procedimiento de autenticación y accede a las operaciones pendientes de autenticar para comprobar que la Parte A tiene una operación pendiente de ser autenticada y, si es correcto, descifra el mensaje según el procedimiento de autenticación, y si entre los datos descifrados está el VRM1 correcto, contrastado con su valor recalculado, será porque el mensaje procede de la aplicación de autenticación de la Parte A ya que es la única que puede haberlos cifrado de la forma recibida, con lo que la Parte A queda autenticada como creadora del mensaje frente a la Parte B, así como el mensaje y su contenido. La AA2 verifica que los datos de la operación recibidos coinciden con los de la operación que tiene pendiente de autenticar y, si es así, da por autenticada y confirmada la operación comunicándolo a la AO. La AO, vía el dispositivo D1A, comunicará a la Parte A dicha confirmación.
- la Parte B enviará un mensaje M2 a la AA1 informándola del resultado de la operación de autenticación que solicitó en su mensaje M1. Para ello la aplicación de autenticación de la Parte B construye un segundo mensaje cifrado M2, según el procedimiento de autenticación simplificado, conteniendo los datos de la operación junto con el resultado de la confirmación y lo envía a la aplicación de autenticación AA1 de la Parte A;

- la aplicación de autenticación de la Parte A recibe el mensaje cifrado M2, lo procesa según el procedimiento de autenticación simplificado, y comprueba que es el VAM2 el valor utilizado para el cálculo del VRM2 con lo que la Parte B queda autenticada como creadora del mensaje frente a la Parte A, pues es la única junto con la Parte A que conoce dicho valor VAM2, y el hecho de que éste M2 es la respuesta al M1 enviado, con lo que se asegura de que su solicitud de autenticación ha sido recibida por la Parte B y ha sido procesada correctamente.

Un esquema de esta operativa y flujo de mensajes queda representado en la Figura 2.

Una aplicación real de esta forma de operar es el caso de un pago realizado con un teléfono móvil en un terminal NFC. Aquí el D1A es el datafono NFC; la AO es la aplicación del banco que trata los pagos realizados en dicho datafono; los DO son los datos de la operación de pago; AA2 es el servidor central de autenticación que forma parte del sistema informático del banco; la AA1 es la aplicación de pagos con NFC soportada por el móvil del usuario, D2A. En este caso, operando de la forma descrita, el banco, a través de su servidor central de autenticación (parte B), sabe que el mensaje M1 con los datos del pago a realizar fue enviado por la aplicación del usuario (parte A) y dicho usuario, al recibir el mensaje M2, sabe que la información que llega viene del servidor central de autenticación (parte B) del banco pues únicamente ellos son los que conocen la clave de descifrado CC utilizada para cifrar el mensaje M1. Además, el servidor central de autenticación sabe que los datos del pago a realizar que le llegaron cifrados en el mensaje M1 son los que el usuario ha validado con la aplicación de su móvil de forma que son los correctos del pago, y si no coinciden con los que el SCA recibió de la aplicación operativa del pagos AO, es que ha habido una interceptación y manipulación de los datos enviados desde el D1A a la AO (posible intento de fraude tipo *man in the middle*) y deben ser rechazados, evitando así el fraude.

Finalmente, se expone un modo de realización preferido. Modo en el que la Parte A solicita la ejecución de una operación a la Parte B y, aplicando el sistema de autenticación objeto de la invención, lleva a cabo una autenticación mutua de las dos Partes y autentica y confirma la operación a ejecutar.

Características

La realización preferente hace uso del procedimiento de autenticación simplificado descrito

en el que se aplican las simplificaciones 2 y 3. Así: únicamente la Parte Central puede dialogar con todas las Parte A, nombre genérico de cada una de las Partes que pueden dialogar con la Parte Central (Parte B), y las Parte A únicamente pueden dialogar con la Parte Central; y el algoritmo de cifrado a usar será el AES.

El sistema de autenticación sólo funcionará correctamente en una aplicación AA específica de cada Parte A y con un código de activación CA también determinado, ya que para la generación de la clave de cifrado CC se hará uso del CA de variables específicas de la AA. Así, aunque alguien copie la AA se encuentra con el problema de desconocer el CA y, por lo tanto, la falta del valor CC necesario para poder operar con ella.

Si a la Parte Central la llamamos Parte B y al resto de Partes las llamamos genéricamente Parte A, las características a destacar en éste diálogo autenticado según el sistema de autenticación son:

- las partes, Parte A y Parte B, están inequívocamente identificadas entre ellas, y con el sistema de autenticación, mediante un primer y segundo identificador;
- la Parte A dispone de, al menos, un primer dispositivo, físico o lógico, (D1A) y un segundo dispositivo, físico o lógico, (D2A) en el que reside una primera aplicación de autenticación (AA1);
- el primer dispositivo de la primera parte D1A con gran frecuencia es un PC, (aunque también puede ser un teléfono móvil, cajero automático, Terminal Punto de Venta físico o lógico, Panel de control IoT, o cualquier otro dispositivo, físico o lógico, con capacidades equivalentes), que pueda solicitar operaciones a un sistema informático y colaborar en su realización en representación de la Parte A.
- el segundo dispositivo de la primera parte D2A normalmente será un teléfono móvil inteligente, aunque también puede ser cualquier otro dispositivo, físico o lógico, con capacidades equivalentes, en el que pueda ejecutarse el software de la aplicación de autenticación AA1;
- para activar dicha primera aplicación de autenticación AA1 la Parte A tendrá que teclear un Código de Activación CA o hacer uso de un medio (huella dactilar de la Parte A, una Tarjeta de Acceso tipo NFC o con un código QR, o cualquier otro medio similar) el cual aportará a la AA1 el Código de Activación CA;
- la Parte B dispone de un dispositivo, físico o lógico, (D1B) en el que reside una segunda aplicación de autenticación (AA2), relacionada inequívocamente, dentro del sistema

de autenticación, con dicha primera aplicación de autenticación AA1. Esta AA2 está activa y se ejecuta en un entorno seguro con las medidas de seguridad necesarias para poder pensar que sólo la Parte B puede tener acceso a la aplicación AA2 y a sus datos;

- dicha Parte B dispone de aplicaciones operativas (AO), soportadas por su sistema informático, con las que la Parte A, desde su primer dispositivo (D1A), puede realizar operaciones relativas a la actividad operativa del sistema informático de la Parte B;
- dicha segunda aplicación de autenticación AA2, de la Parte B, forma parte del sistema informático de la Parte B y se relaciona con sus aplicaciones operativas AO (figura 1);
- dicha segunda aplicación de autenticación de la Parte B se puede relacionar con tantas aplicaciones de autenticación de Partes A como usuarios tenga el sistema informático de la Parte B;
- dichas primera y segunda aplicación, AA1 y AA2, disponen cada una de ellas de un identificador único dentro del sistema de autenticación, IdA e IdB respectivamente;
- dichas primera y segunda aplicación comparten una misma clave de cifrado CC que usarán a lo largo del procedimiento de autenticación mutua;
- dicha primera aplicación, AA1, dispone de un algoritmo generador de números pseudoaleatorios;
- dichas primera y segunda aplicación, AA1 y AA2, disponen cada una de ellas del mismo algoritmo de cifrado AES 128, o cualquier otro de características similares, para sus operaciones de cifrado/descifrado;
- la AA2 tendrá tantos diferentes valores de clave de Cifrado CC como aplicaciones de autenticación de Partes A estén relacionadas con ella;
- los dispositivos de dichas Parte A y Parte B están en comunicación por medio de uno o más canales de comunicación, físicos o lógicos, diferentes;
- opcionalmente, todos los mensajes que se intercambian las Partes A y B son guardados por el sistema de autenticación en un fichero para su posterior uso como fichero de registro de la actividad del sistema (LOG).

Operativa

- la Parte A por medio de su primer dispositivo D1A solicita la ejecución de una operación a una de las aplicaciones operativas (AO) de la Parte B;
- la aplicación operativa AO recibe del dispositivo de la Parte A, D1A, la solicitud de operación con los datos de la operación DO que deberán ser autenticados y autorizados por la Parte A desde su Aplicación de Autenticación AA1 debido a la falta de seguridad del canal por el que se ha recibido la solicitud y a la necesidad de confirmación que requiere la ejecución

de la operación;

- la aplicación operativa AO prepara los datos de la operación DO recibidos y los envía a la aplicación de autenticación de la Parte B, AA2, la cual los recibe y deja a la espera de que sean autenticados por la Parte A;
- la Parte A activa en su D2A su aplicación de autenticación AA1 aportando el código de activación CA;
- la Parte A con su aplicación de autenticación AA1 es la que envía un primer mensaje cifrado M1, según el procedimiento de autenticación, a la aplicación de autenticación de la Parte B indicando que quiere autenticar una operación que la Parte A le ha solicitado, desde su primer dispositivo D1A, y que la Parte B debe tener pendiente de autenticar. Entre los datos de la operación que viajan cifrados estará la dirección del Emisor del mensaje dentro de la red por la que se comunica;
- la aplicación de autenticación de la Parte B, AA2, recibe dicho primer mensaje M1 cifrado según el procedimiento de autenticación y accede a las operaciones pendientes de autenticar para comprobar que la Parte A tiene una operación pendiente de ser autenticada y, si es correcto, descifra el mensaje según el procedimiento de autenticación, y si entre los datos descifrados está el VRM1 correcto, contrastado con su valor recalculado, será porque el mensaje procede de la aplicación de autenticación de la Parte A ya que es la única que puede haberlos cifrado de la forma recibida, con lo que la Parte A queda autenticada como creadora del mensaje frente a la Parte B así como el mensaje y su contenido. En el caso en que no encuentre una operación esperando a ser autenticada, la AA2 guardará el mensaje, durante un tiempo corto preestablecido, a la espera de que llegue de la AO una operación de la Parte A y que necesite ser autenticada (lógicamente en un momento determinado para una misma Parte A no puede haber más de una operación en espera de que lleguen los otros datos que necesita para iniciar su tramitación);
- una vez verificado el que los datos de la operación en espera son compatibles con la información que le ha llegado a la AA2, ésta construye un segundo mensaje cifrado M2, según el procedimiento de autenticación, conteniendo los datos de la operación pendiente de autenticación y lo envía a la aplicación de autenticación de la Parte A;
- la aplicación de autenticación de la Parte A recibe el mensaje cifrado M2, lo descifra según el procedimiento de autenticación y comprueba la validez del VAM2 con lo que la Parte B queda autenticada como creadora del mensaje frente a la Parte A, así como el mensaje y su contenido, y el hecho de que éste M2 es la respuesta al M1 enviado. Entonces la AA1 presenta los datos de la operación a la Parte A en su dispositivo D2A para que verifique que se corresponden con los de la operación que él ha solicitado desde su dispositivo D1A y, si

es así, autorice, o no, la operación. Para comunicar su decisión crea el mensaje M3, según el procedimiento de cifrado y autenticación, con los datos de la operación y el resultado de la autorización para enviarlo a la aplicación de autenticación de la Parte B;

- la aplicación de autenticación de la Parte B recibe dicho mensaje cifrado M3 y lo trata según el procedimiento de autenticación, y si entre los datos descifrados está el VAM3 que le corresponde será porque el mensaje procede de la aplicación de autenticación de la Parte A ya que es la única que puede haberlos cifrado de la forma recibida, con lo que la Parte A queda autenticada como creadora del mensaje frente a la Parte B así como el mensaje y su contenido, y el hecho de que éste M3 es la respuesta al M2 enviado. Verifica que los datos de la operación a autorizar concuerdan con los que tiene pendiente de autenticar/confirmar y comunica a la Aplicación Operativa, AO, de la Parte B el resultado de la autenticación y autorización de la operación realizada por la Parte A. Opcionalmente, envía un mensaje M4 a la aplicación de autenticación de la Parte A, AA1, para que informe a la Parte A de la finalización de la operación;
- la aplicación operativa de la Parte B enviará un mensaje al dispositivo D1A de la Parte A comunicándole el resultado de la operación;

Un esquema de esta operativa y flujo de mensajes queda representado en la Figura 3.

Una aplicación real de esta forma de operar es el caso de la realización de una transferencia en la banca online. Aquí el D1A es el PC desde el que se opera con la banca online; la AO es la aplicación del banco que trata la operativa de las operaciones de transferencias; los DO son los datos de la transferencia; AA2 es el servidor central de autenticación que forma parte del sistema informático del banco; la AA1 es la aplicación de autenticación soportada por el móvil del usuario, D2A.

En este caso, operando de la forma descrita, el banco, a través de su servidor central de autenticación SCA, sabe que el mensaje M1 fue enviado por la aplicación del usuario Parte A y dicho usuario, al recibir el mensaje M2 sabe que los datos de la transferencia que le llegan vienen del servidor central de autenticación SCA del banco, pues únicamente ellos son los que conocen la clave de descifrado CC utilizada para cifrar el mensaje M1. Además el SCA sabe que los datos de la transferencia a realizar que le llegaron cifrados en el mensaje M3 son los que el usuario ha validado con la aplicación de su móvil, de forma que son los correctos. Si el usuario hubiera rechazado la operación porque los datos de la transferencia recibidos en el M2 no coinciden con los que solicitó desde el D1A, será porque ha habido una

interceptación y manipulación de los datos enviados desde el D1A a la AO (posible intento de fraude tipo *man in the middle*) ya que es la única comunicación que no viajó cifrada y, por lo tanto, es susceptible de ser manipulada.

Descrita suficientemente la naturaleza de la presente invención, así como la manera de ponerla en práctica, no se considera necesario hacer más extensa su explicación para que cualquier experto en la materia comprenda su alcance y las ventajas que de ella se derivan, haciéndose constar que, dentro de su esencialidad, podrá ser llevada a la práctica en otras formas de realización que difieran en detalle de la indicada a título de ejemplo, y a las cuales alcanzará igualmente la protección que se recaba siempre que no se altere, cambie o modifique su principio fundamental.

REIVINDICACIONES

1.- Procedimiento para el cifrado y autenticación de comunicaciones, con autenticación mutua de los comunicantes, que está **caracterizado** porque cada una de las Partes en comunicación, Parte A y Parte B, dispone de una Aplicación de Autenticación (AA), en un dispositivo hardware/software, que les permite el intercambio de mensajes entre ellas, siendo que cada Aplicación de Autenticación dispone de:

- su Identificador, que la identifica de forma inequívoca frente al resto de Aplicaciones de Autenticación integradas en el Sistema de Autenticación;
- los Identificadores de cada una de las Aplicaciones de Autenticación de otras Partes que estén definidas como sus posibles interlocutores dentro del Sistema de Autenticación;
- un valor, diferente para cada pareja de interlocución, a usar como Clave de Cifrado CC de mensajes;
- uno o más canales de comunicación con entre las Partes, a través de los que las aplicaciones de autenticación se intercambian los mensajes;
- un generador de Valores Pseudoaleatorios;
- un algoritmo de cifrado, que comparte con el resto de las Partes del Sistema, que permite cifrar y descifrar los mensajes que se envían/reciben;
- una función resumen, que comparte con el resto de las Partes del Sistema, que permite obtener valores resumen.

caracterizado porque:

la Aplicación de la Parte A:

- genera y guarda dos Valores Pseudoaleatorios, VAM2 y VAM3 a usar como Valores de Autenticación (VAMx) en los mensajes M2 y M3 respectivamente
- prepara la información a enviar conteniendo, al menos, los valores IdA, IdB, VAM2, VAM3 y DATOS1, donde DATOS1 contendrá información que se desee comunicar a

la Parte B; aplica a ésta información una función resumen, que comparten Parte A y Parte B, obteniendo un Valor Resumen de la información a transmitir en el mensaje M1, VRM1; cifra, aplicando el algoritmo de cifrado que comparten Parte A y Parte B, con CC, obteniendo CC(VAM2, VAM3, DATOS1, VRM1).

- envía a la Aplicación de la Parte B un mensaje M1 conteniendo, entre otros, los datos: IdB; IdA; CC (VAM2, VAM3, DATOS1, VRM1);

que la Aplicación de la Parte B:

- recibe el mensaje M1,
- verifica el Identificador de Parte A,
- descifra con CC el CC (VAM2, VAM3, DATOS1, VRM1); aplica la misma función resumen a los mismos valores recibidos (IdB, IdA, VAM2, VAM3, DATOS1), y obtiene el Valor Resumen que debe tener el VRM1 recibido; en que, en el caso en que si coincide el VRM1 calculado con el recibido, es que el descifrado ha sido realizado correctamente luego el que creó el mensaje y realizó el cifrado ha sido la Parte A, y entonces:
- guarda los valores VAM2, VAM3 para su posterior uso;
- compone el mensaje IdA, IdB, DATOS2, VAM2, con los DATOS2 a enviar, y calcula su valor resumen VRM2 aplicando la misma función resumen;
- envía a la Parte A (IdA) un mensaje M2 conteniendo, entre otros posibles valores, los de: IdA, IdB, DATOS2, VRM2;

que la Aplicación de la Parte A:

- recibe de la Aplicación de la Parte B el mensaje M2;
- verifica el Identificador de Parte B;
- recalcula el valor de VRM2 sobre los datos IdA, IdB, DATOS2, VAM2M1, donde el valor VAM2M1 es el VAM2 enviado en el mensaje M1 y verifica su coincidencia con el VRM2 recibido; en que, en el caso en que si coincide es que quien calculó el VRM2 recibido es la Parte B, pues sólo ella dispone del valor VAM2, con lo que ya las dos partes saben con quién están dialogando, y entonces, opcionalmente;
- compone el mensaje IdB, IdA, DATOS3, VAM3, con los DATOS3 a enviar, y calcula su función resumen VRM3;
- envía a la Parte B (IdB) un mensaje M3 conteniendo, entre otros posibles valores, los

de: IdB, IdA, DATOS3, VRM3.

y que la Aplicación de la Parte B:

- recibe el mensaje M3 con IdB, IdA, DATOS3, VRM3;
- verifica el Identificador de Parte A;
- recalcula el valor de VRM3 sobre los datos IdA, IdB, DATOS3, VAM3M1 donde el valor VAM3M1 es el VAM3 recibido en el mensaje M1 y verifica su coincidencia con el VRM3 recibido; en que, en el caso en que si coincide es que quien calculó el VRM3 recibido es la Parte B, pues sólo ella dispone del valor VAM3, y entonces el mensaje M3 es la respuesta autenticada al M2.

2.- Procedimiento para el cifrado y autenticación de comunicaciones, con autenticación mutua de los comunicantes, según la reivindicación 1, **caracterizado** porque, cuando es necesario que la parte A sepa que su mensaje M3 llegó a la parte B, en el mensaje M1 se envía un valor VAM4 y la aplicación de la parte B procede a componer un mensaje M4 para ser enviado a la aplicación de la parte A.

3.- Procedimiento para el cifrado y autenticación de comunicaciones, con autenticación mutua de los comunicantes, según reivindicación 1, **caracterizado** porque:
la aplicación de la Parte A:

- genera y guarda cuatro Valores Pseudoaleatorios, CCM2, VAM2 y CCM3, VAM3 a usar como Claves de Cifrado (CCMx) de los mensajes y Valores de Autenticación (VAMx) en sendos mensajes M2 y M3 respectivamente;
- aplica una función resumen para calcular el Valor Resumen, VRM1, de los identificadores de la Aplicación de la Parte A y de la Parte B, los valores generados y otros datos que interese comunicar;
- envía a la aplicación de la Parte B un mensaje M1 conteniendo, entre otros posibles valores, los identificadores de la Aplicación de la Parte A y de la Parte B junto con el valor cifrado, con la clave de cifrado CCAB, de los valores generados, los datos que interese comunicar y el valor VRM1;

la aplicación de la Parte B:

- recibe el mensaje M1, verifica el Identificador de la aplicación de la Parte A y descifra con CCAB la parte cifrada obteniendo, entre otros, el valor VRM1;
- aplica, como hizo la Parte A, la misma función resumen a los mismos valores recibidos y obtiene su Valor Resumen que debe coincidir con el VRM1 recibido; en el caso en que si coinciden los VRM, es que el mensaje fue enviado por la aplicación de la parte A, y entonces;
- para su posterior uso guarda los valores CCM2, VAM2, CCM3, VAM3;
- envía a la aplicación de la Parte A un mensaje M2 conteniendo, entre otros posibles valores, los identificadores de la Aplicación de la Parte A y de la Parte B junto con el valor cifrado, con la clave de cifrado CCM2, del valor VAM2 y los datos que interese comunicar;

la aplicación de la Parte A:

- recibe de la aplicación de la Parte B el mensaje M2, verifica el Identificador de la aplicación de la Parte B y descifra con CCM2 la información del M2 para obtener el VAM2 y verificar su coincidencia con el enviado en el M1, en que, en el caso en que si coinciden los VAM, es que el mensaje fue enviado por la aplicación de la parte B, con lo que ya las dos partes saben con quién están dialogando, y entonces, opcionalmente,
- envía a la aplicación de la Parte B (IdB) un mensaje M3 conteniendo, entre otros posibles valores, los identificadores de la Aplicación de la Parte A y de la Parte B junto con el valor cifrado, con la clave de cifrado CCM3, del valor VAM3 y los datos que interese comunicar;

y la aplicación de la Parte B:

- recibe de la aplicación de la Parte A el mensaje M3, verifica el Identificador de la aplicación de la Parte A y descifra con CCM3 la información cifrada para obtener el VAM3 y verificar su coincidencia con el recibido en el M1; en que, en el caso en que si coinciden los VAM, es que el mensaje M3 fue enviado por la aplicación de la parte A como respuesta a su M2.

4.- Procedimiento para el cifrado y autenticación de comunicaciones, con autenticación mutua de los comunicantes, según la reivindicación 1, caracterizado porque el valor de la clave de

cifrado CCAB, que se usa en el cifrado y descifrado del mensaje M1, es diferente para cada diálogo en el que la Parte A y Parte B se intercambian los mensajes M1 y M2, que comprende: que la aplicación de la Parte A:

- genera y guarda cuatro Valores Pseudoaleatorios, CCM2, VAM2 y CCM3, VAM3 a usar como Claves de Cifrado (CCMx) de los mensajes y Valores de Autenticación (VAMx) en sendos mensajes M2 y M3 respectivamente;
- aplica una función resumen para calcular el Valor Resumen, VRM1, de los identificadores de la Aplicación de la Parte A y de la Parte B, los valores generados, datos que interese comunicar y el valor del dato RecibidoM2AB, siendo que RecibidoM2AB contendrá el valor Si o NO para indicar a la Aplicación de la Parte B si en el ultimo diálogo iniciado por Parte A, la Parte A recibió el mensaje M2 de la Parte B de forma que la Parte B pueda actuar en consecuencia.
- envía a la aplicación de la Parte B un mensaje M1 conteniendo, entre otros posibles valores, los identificadores de la Aplicación de la Parte A y de la Parte B, el valor de RecibidoM2AB y el valor cifrado, con la clave de cifrado CCAB, de los cuatro valores generados, los datos que interese comunicar y el valor VRM1;
- una vez enviado el M1 guarda el valor NO en el dato RecibidoM2AB para indicar que Parte A ha iniciado un diálogo con Parte B pero todavía no ha recibido el mensaje M2 de dicho diálogo;

que la aplicación de la Parte B:

- recibe el mensaje M1, verifica el Identificador de la aplicación de la Parte A y descifra con CCAB la parte cifrada obteniendo, entre otros, el valor VRM1;
- aplica, como hizo la Parte A, la misma función resumen a los mismos valores recibidos y obtiene su Valor Resumen que debe coincidir con el VRM1 recibido y:
- en el caso en que si coinciden los VRM, es que el mensaje fue enviado por la aplicación de la parte A, y entonces;
- para su posterior uso guarda los valores CCM2, VAM2, CCM3, VAM3;
- genera un valor CCSIG a emplear como clave de cifrado del mensaje M1 del próximo diálogo que vaya a tener la Parte B con la Parte A y lo almacena en el dato CCSIGAB;
- envía a la aplicación de la Parte A (IdA) un mensaje M2 conteniendo, entre otros posibles valores, los identificadores de la Aplicación de la Parte A y de la Parte B junto

con el valor cifrado, con la clave de cifrado CCM2, del valor VAM2, los datos que interese comunicar, y el valor CCSIGAB;

- se guarda el valor de CCAB en el dato CCUUAB por si en un siguiente diálogo fuera necesario reutilizar el valor de CCAB para descifrar el M1 recibido;
- se guarda el valor de CCSIGAB en el dato CCAB que, inicialmente, se usará para descifrar el próximo M1 que le llegue.
- en el caso en que no coinciden los VRM, entonces:
- verifica si el dato RecibidoM2AB tiene el valor NO y en el caso en que no es así es que ha habido un error o intento de ataque al sistema.
- en el caso en que RecibidoM2AB tenga el valor NO entonces:
- guarda el valor de CCUUAB en CCAB, de forma que se use como clave de descifrado del M1 la misma que se usó para descifrar el anterior M1 recibido. Esto sucede siempre que la Parte A no haya recibido el M2 del anterior diálogo con la nueva clave de cifrado a usar en la variable CCSIGAB;
- descifra de nuevo con CCAB;
- aplica, como hizo la Parte A, la misma función resumen a los mismos valores recibidos y obtiene su Valor Resumen VRM1R y comprueba si coincide con el VRM1 recibido;
- en el caso en que no coincide es que ha habido un error o intento de ataque al sistema;
- en el caso en que si coinciden es que la Parte A es la emisora del M1 y entonces:
- para su posterior uso guarda los valores CCM2, VAM2, CCM3, VAM3 y genera un valor CCSIG que lo almacena en CCSIGAB;
- envía a la aplicación de la Parte A (IdA) un mensaje M2 conteniendo, entre otros posibles valores: los identificadores de la Aplicación de la Parte A y de la Parte B junto con el valor cifrado, con la clave de cifrado CCM2, del valor VAM2, los datos que interese comunicar, y el valor CCSIGAB:
- una vez enviado el M2 se guarda el valor de CCAB en el dato CCUUAB y se guarda el valor de CCSIGAB en el dato CCAB.

que la aplicación de la Parte A:

- recibe de la aplicación de la Parte B el mensaje M2, verifica el Identificador de la aplicación de la Parte B y descifra con CCM2 la información del M2 para obtener el VAM2 y verificar su coincidencia con el enviado en el M1, en que:

- en el caso en que si coinciden los VAM, es que el mensaje fue enviado por la aplicación de la parte B, con lo que ya las dos partes saben con quién están dialogando, y entonces;
- guarda en CCAB el valor del CCSIGAB recibido;
- guarda el valor SI en RecibidoM2AB;
- opcionalmente, envía a la aplicación de la Parte B un mensaje M3 conteniendo, entre otros posibles valores, los identificadores de la Aplicación de la Parte A y de la Parte B junto con el valor cifrado, con la clave de cifrado CCM3, del valor VAM3 y los datos que interese comunicar;

y que la aplicación de la Parte B:

- recibe de la aplicación de la Parte A el mensaje M3, verifica el Identificador de la aplicación de la Parte A y descifra con CCM3 la información cifrada para obtener el VAM3 y verificar su coincidencia con el recibido en el M1; en que, en el caso en que si coinciden los VAM, es que el mensaje M3 fue enviado por la aplicación de la parte A como respuesta a su M2.

5.- Procedimiento para el cifrado y autenticación de comunicaciones, con autenticación mutua de los comunicantes, según la reivindicación 3 o 4, caracterizado porque, cuando es necesario que la parte A sepa que su mensaje M3 llegó a la parte B, entonces en el mensaje M1 se envía un valor CCM4 y VAM4 y la aplicación de la parte B procede a componer un mensaje M4 para ser enviado a la aplicación de la parte A.

6.- Procedimiento para el cifrado y autenticación de comunicaciones, con autenticación mutua de los comunicantes, según cualquiera de las reivindicaciones 1, 3 ó 4, caracterizado porque el diálogo se inicia automáticamente entre las dos Aplicaciones de Autenticación AAA y AAB, de las Partes A y B, cuando a la AAA le llega un evento esperado, siendo que las Aplicaciones de Autenticación están previamente activas y disponen de la clave de cifrado CCAB que comparten.

7.- Procedimiento para el cifrado y autenticación de comunicaciones, con autenticación mutua de los comunicantes, según cualquiera de las reivindicaciones 1, 3 ó 4, caracterizado porque la activación de una aplicación AA se realiza aportando la Parte, persona usuaria de la

aplicación, un código de activación CA que será el segundo factor de autenticación de dicha Parte persona física dentro del diálogo.

8.- Procedimiento para el cifrado y autenticación de comunicaciones, con autenticación mutua de los comunicantes, según la reivindicación 7, caracterizado porque, para que una aplicación AA valide un mensaje M enviado por la otra aplicación que interviene en el diálogo, la Parte, persona usuaria de la aplicación, necesita aportar un valor que será el tercer factor de autenticación de dicha Parte persona física dentro del diálogo.

9.- Sistema para el cifrado y autenticación de comunicaciones, con autenticación mutua de los comunicantes, que está caracterizado porque cada una de las Partes en comunicación, Parte A y Parte B, dispone de una Aplicación de Autenticación (AA), en un dispositivo hardware/software, que les permite el intercambio de mensajes entre ellas, siendo que cada Aplicación de Autenticación dispone de:

- su Identificador, que la identifica de forma inequívoca frente al resto de Aplicaciones de Autenticación integradas en el Sistema de Autenticación;
- los Identificadores de cada una de las Aplicaciones de Autenticación de otras Partes que estén definidas como sus posibles interlocutores dentro del Sistema de Autenticación;
- un valor, diferente para cada pareja de interlocución, a usar como Clave de Cifrado CC de mensajes;
- uno o más canales de comunicación con entre las Partes, a través de los que las aplicaciones de autenticación se intercambian los mensajes;
- un generador de Valores Pseudoaleatorios;
- un algoritmo de cifrado, que comparte con el resto de las Partes del Sistema, que permite cifrar y descifrar los mensajes que se envían/reciben;
- una función resumen, que comparte con el resto de las Partes del Sistema, que permite obtener valores resumen.

estando configurado cada elemento del sistema para la ejecución del procedimiento según una cualquiera de las reivindicaciones 1-8.

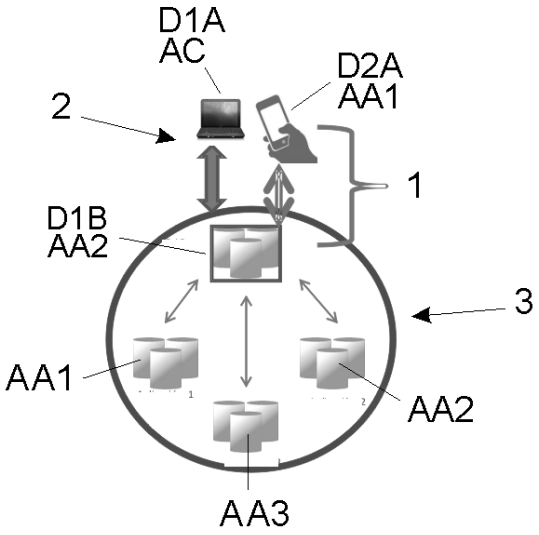
D1A
AC
D2A
AA1
2
1
D1B
AA2
3
AA1
AA2
AA3

FIG. 1

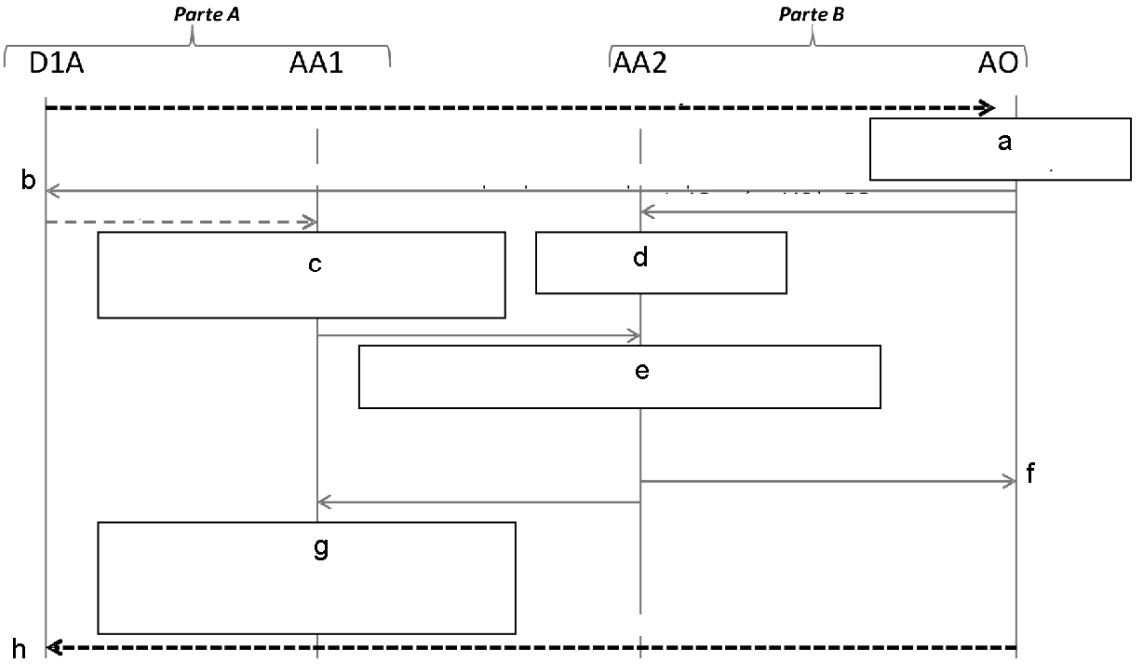
Parte A
Parte B
D1A
AA1
AA2
AO
a
b
c
d
e
f
g
h

FIG. 2

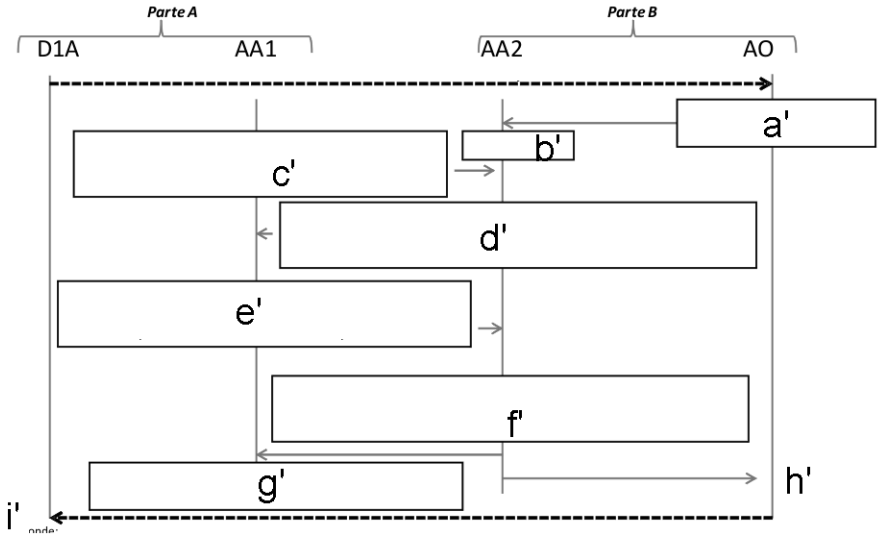
Parte A
Parte B
D1A
AA1
AA2
AO
a'
b'
c'
d'
e'
f'
g'
h'
i'

FIG. 3

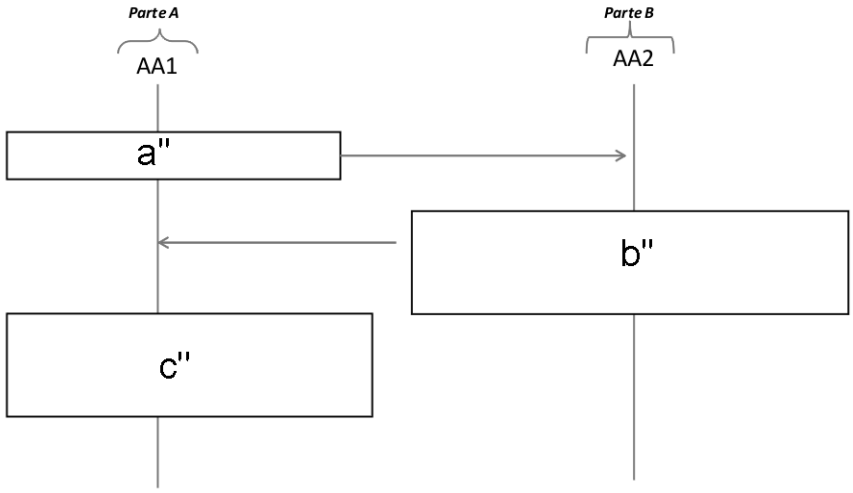
Parte A
Parte B
AA1
AA2
a''
b''
c''

FIG. 4

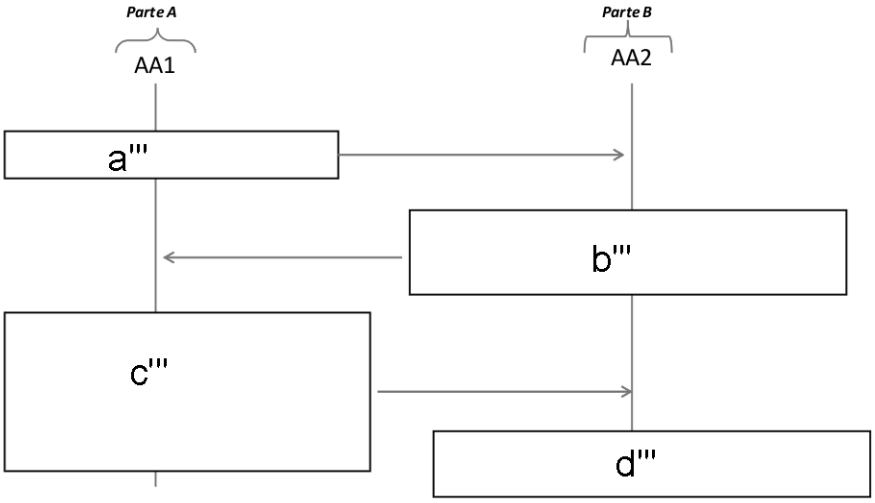

FIG. 5