(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 537 172**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.06.2010 E 10727732 (9)**

(97) Fecha y número de publicación de la concesión europea: **17.12.2014 EP 2452478**

(54) Título: **Procedimiento de gestión de una aplicación integrada en un dispositivo electrónico asegurado**

(30) Prioridad:

09.07.2009 EP 09305663

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.06.2015

(73) Titular/es:

GEMALTO SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

GALLAS, FREDERIC;
AMIEL, PATRICE y
BERARD, XAVIER

(74) Agente/Representante:

ISERN CUYAS, María Luisa

DESCRIPCIÓN

Procedimiento de gestión de una aplicación integrada en un dispositivo electrónico asegurado.

La presente invención hace referencia a métodos de gestión de una aplicación integrada en un token electrónico asegurado. Hace referencia particularmente a métodos de administración de aplicaciones que están integradas en tarjetas con chip.

(Técnica anterior)

Un token electrónico asegurado como una tarjeta con chip, también denominada tarjeta inteligente, puede contener aplicaciones en forma de applets. Se puede acceder a estos applets por un servidor remoto mediante un canal aéreo, conocido como OTA. El mecanismo OTA se define por los estándares ETSI SCP 102.225, ETSI-SCP 102.226 y GlobalPlatform 2.2 para RAM. El canal OTA permite acceder a datos y aplicaciones que han sido específicamente desarrollados para tarjetas SIM. Solamente las tarjetas cuyo uso se ha diseñado para un dominio Telecom o en un dominio Máquina a Máquina (M2M) pueden administrar una comunicación OTA. Concretamente las tarjetas SIM ofrecen características OTA. Puede accederse a estas tarjetas con chip a través del Protocolo de Transferencia de Hipertexto, normalmente llamado HTTP. En particular, las versiones estándar 1.0 y posteriores de OMA-SCWS definen un protocolo de administración para la administración OTA de los recursos del Servidor Web de Tarjetas Con Chip (SCWS). Este protocolo se basa en un mensaje POST HTTP enviado por una aplicación de Agente Administrador al servidor OTA. La aplicación de Agente Administrador se encuentra en la tarjeta con chip. Como respuesta, el servidor OTA envía de vuelta un comando de administración SCWS en el cuerpo de la respuesta POST HTTP. Según el estándar, un Tipo de Contenido fijo es especificado en la cabecera de esta respuesta HTTP POST. A la recepción de este mensaje, y gracias al Tipo de Contenido, la aplicación de Agente Administrador reenvía el cuerpo de la respuesta HTTP POST al SCWS para la ejecución de los comandos de administración que contiene. Entonces, una vez los comandos administrativos han sido ejecutados por el SCWS, otra solicitud HTTP POST es enviada por la aplicación de Agente Administrador con el propósito de notificar al servidor OTA los resultados de la ejecución de los comandos. Estos datos de resultados se introducen en un mensaje HTTP POST, y un Tipo de Contenido específico es colocado en la cabecera de este HTTP POST. Usando un principio similar, el GlobalPlatform ® 2.2 estándar (Enmienda B "RAM sobre HTTP") ha definido un protocolo de administración para la administración del OTA del contenido de la tarjeta con chip. Este canal se adapta bien al mecanismo Gestión Remota de Applet (RAM), para la administración de Dominios de Seguridad, paquetes y applets. El GlobalPlatform ® 2.2 estándar especifica un patrón fijo de Tipo de Contenido a emplear en los mensajes de solicitud HTTP POST y en los mensajes de respuesta HTTP POST.

La mayoría de las aplicaciones desarrolladas para las tarjetas SIM son diseñadas con una Interfaz de programación de Aplicaciones (API) capaz de administrar el canal OTA. Dichas aplicaciones de tarjetas con chip no son capaces de administrar el canal HTTP. En la actualidad no es posible dirigirse a estas aplicaciones ya que la ruta de la respuesta HTTP tiene que estar garantizada por el Agente Administrador que no es consciente de los valores específicos de Tipo de Contenido exceptuando OMA-SCWS, RAM en HATTP y RFM en HTTP. En los tres estándares mencionados anteriormente, la aplicación de Agente Administrador es un componente clave para la administración de estos protocolos "OPA sobre HTTP". Además, la aplicación del Agente Administrador forma generalmente parte del Sistema Operativo de las tarjetas con chip. Como consecuencia, no resulta fácilmente posible modificar su comportamiento.

Existe la necesidad de reutilizar el mismo protocolo "OTA sobre HTPP" para motivos distintos de la administración de recursos SCWS y administración del contenido de la Tarjeta como se define por GlobalPlatform ® o los estándares ETSI. En particular, existe una necesidad de acceso a cualquier aplicación integrada en una tarjeta con chip mediante el mecanismo HTTP. En particular un servidor lejano debe poder comunicarse con una aplicación integrada en una tarjeta con chip mediante una sesión HTTP para personalizar la aplicación o utilizar un servicio suministrado por la aplicación.

La WO2006/061754 revela un sistema y un método de transferencia de derechos de administración de tarjetas con chip de una parte a otra.

(Sumario de la invención)

El objeto de la invención es resolver el problema técnico mencionado anteriormente.

El objeto de la presente invención es un método de administrar una aplicación que está integrada en un token electrónico asegurado. El token electrónico asegurado está diseñado para recibir un mensaje desde una máquina de servidor. El token electrónico asegurado comprende un agente capaz de administrar dicho mensaje. El mensaje tiene una cabecera y un cuerpo. El método comprende las etapas de:

a) registro de la aplicación en el agente mediante la asociación de una referencia de la paliación con un valor de un elemento de la cabecera del mensaje,

b) cuando se recibe el mensaje de la máquina de servidor, transfiere parte de dicho mensaje a la aplicación si la cabecera del mensaje contiene un elemento que posee el valor asociado a la referencia de la aplicación.

Provechosamente, cuando la aplicación puede generar una respuesta al mensaje y el método puede comprender la etapa de envío de dicha respuesta a la máquina del servidor.

En una realización preferida, el mensaje puede cumplir el formato HTTP o HTTPS.

Provechosamente, el elemento de la cabecera puede ser un Tipo de Contenido como se define por el estándar HTTP-RFC 2616 HTTP/1.

En una realización preferida, el agente puede rechazar la etapa de registro si la aplicación no cumple con las reglas preestablecidas de seguridad.

Provechosamente, el agente puede rechazar la etapa de registro si el valor de dicho elemento se encuentra ya registrado en otra aplicación.

La etapa de registro puede ser solicitada por la aplicación.

Provechosamente, el token electrónico asegurado puede comprender una segunda aplicación y la etapa de registro puede ser solicitada por la segunda aplicación.

Alternativamente, la etapa de registro puede ser solicitada por la máquina del servidor.

Otro objeto de la invención es un token electrónico asegurado diseñado para recibir un mensaje de la máquina del servidor. El token electrónico asegurado comprende un agente capaz de administrar el mensaje. El mensaje tiene una cabecera y un cuerpo. El token electrónico asegurado comprende: un microprocesador, una interfaz de comunicación, un sistema operativo, una memoria de trabajo y una memoria no volátil. El token electrónico asegurado está diseñado para comprender una aplicación, un primer y segundo medio. El primer medio es capaz de registrar la aplicación asociando una referencia de la aplicación con un valor de un elemento de la cabecera del mensaje. El segundo medio es capaz de transferir parte del mensaje a la aplicación si la cabecera del mensaje contiene un elemento que tiene el valor asociado a la referencia de la aplicación.

Provechosamente, el agente puede comprender un tercer medio capaz de verificar si la aplicación cumple con las reglas de seguridad preestablecidas, y capaz de rechazar el registro de la aplicación en caso de una verificación insatisfactoria.

En una realización preferida, la aplicación puede generar una respuesta al mensaje y el agente puede comprender un cuarto medio capaz de enviar dicha respuesta a la máquina del servidor.

Provechosamente, la aplicación puede comprender un quinto medio capaz de solicitar al agente el registro de la aplicación.

En una realización preferida, el mensaje puede cumplir con el formato HTTP o HTTPS y el elemento de cabecera puede ser un Tipo de Contenido como se define por el estándar HTTP – RFC 2616 HTTP/1.1.

En una realización preferida, el token electrónico asegurado puede ser una tarjeta con chip.

(Breve descripción de los dibujos)

Otras características y ventajas de la presente invención aparecerán con mayor claridad a lo largo de la lectura de la siguiente descripción de un número de realizaciones preferidas de la invención con referencia a los correspondientes esquemas que acompañan en los cuales:

- La Figura 1 representa de forma esquemática un ejemplo de la arquitectura de un token electrónico asegurado que comunica con un servidor lejano mediante una máquina anfitriona según la invención;
- La Figura 2 es un ejemplo de una primera realización del registro integrado en el agente según la invención;
- La Figura 3 es un ejemplo de arquitectura de agente según la invención; y
- La Figura 4 es un ejemplo de una segunda realización de un registro integrado en el agente según la invención.

(Descripción detallada de las realizaciones preferidas)

La invención puede aplicarse a cualquier tipo de token electrónico asegurado. En particular, la presente invención puede ser aplicada también para asegurar el token electrónico utilizando un Protocolo de Transferencia de Hipertextos Seguro, normalmente denominado HTTPS. En esta especificación, el token electrónico asegurado es una tarjeta SIM pero podría ser otra clase de dispositivo electrónico asegurado capaz de emplear mecanismos HTTP o HTTPS. Un token electrónico asegurado puede ser portátil y puede contener una o varias memorias, un microprocesador y una interfaz de comunicación. En esta especificación, el token electrónico asegurado está conectado a una máquina anfitriona. En particular, la máquina anfitriona puede ser un teléfono móvil o un terminal de telecomunicaciones. El token electrónico accede al servidor remoto mediante la máquina anfitriona. Alternativamente, los mensajes HTTPS pueden ser intercambiados directamente entre el token electrónico seguro y la máquina del servidor sin ninguna máquina anfitriona intermedia.

La presente invención se basa en un agente que permite el registro de una aplicación. Tanto el agente como la aplicación están almacenados en el token electrónico seguro. Un servidor lejano envía un mensaje con una cabecera y un cuerpo. El cuerpo del mensaje está diseñado para ser recibido por la aplicación registrada. Una vez registrado, la aplicación está asociada a un valor específico de un campo de cabecera. Según la invención, el agente es una aplicación mejorada de un Agente Administrador. Cuando recibe un mensaje del servidor lejano el agente es capaz de enviar una parte de este mensaje a la aplicación correspondiente.

Gracias a la invención, el servidor lejano siempre emplea el mecanismo estándar HTTP y permanece totalmente independiente de los límites de la interfaz de la aplicación en cuestión. El agente administra las cuestiones y el formateo de datos para la aplicación a la cual va dirigida.

Una ventaja de la invención es evitar la actualización de la terminal de telecomunicaciones empleada. Tal actualización es muy pesada de administrar y costosa ya que el número de terminales de telecomunicaciones en el campo es enorme. Además existen muchas clases diferentes de teléfonos móviles ya desplegados.

Otra ventaja de la invención es permitir a la aplicación integrada emplear un conjunto específico de comandos y respuestas. El conjunto especifico de comandos y respuestas pueden satisfacer cualquier formato.

Otra ventaja de la invención es evitar el despliegue de varias aplicaciones básicas de Agente Administrador en un único token. Dicho despliegue de varios agentes consume memoria y requiere una validación muy pesada, auditorias y certificaciones en relación a cuestiones de seguridad.

Otra ventaja de la invención es permitir la mezcla de la administración de varios asuntos OTA en una única sesión HTTP OTA. Por ejemplo la invención permite mezclar una operación de Activación con una operación de rastreo IMEI.

Otra ventaja de la invención es permitir que el servidor lejano envíe mensajes que no contiene el Identificador Applet (AID) del applet en cuestión.

Otra ventaja de la invención es permitir el acceso OTA a aplicaciones que han sido descargadas tras la emisión de la tarjeta sin efecto alguno en el Agente Administrador. En otras palabras, las aplicaciones que son descargadas en una etapa de post-personalización pueden obtenerse mediante el canal OTA incluso si el Agente Administrador continua sin cambios.

La **Figura 1** muestra la arquitectura de un identificar electrónico seguro SC de tipo tarjeta SIM según una realización preferida de la invención.

El token electrónico seguro SC comprende una memoria de trabajo MEM1 de tipo RAM, dos memorias no volátiles MEM2 y MEM3, un microprocesador MP y una interfaz de comunicación IN. La memoria no volátil MEM2 comprende un sistema operativo OS que puede contener una máquina Java Virtual.

La memoria no volátil MEM3 comprende dos applets AP1 y AP2, un servidor web de tarjeta con chip SCWS, un dominio de seguridad SD y un agente AA. El dominio de seguridad SD cumple con el estándar GlobalPlatform.

Las dos memorias MEM2 y MEM3 pueden implementarse como combinaciones de una, dos o más memorias. Dichas memorias pueden ser flash de tipo NAND o memoria EEP-ROM u otro tipo de memoria no volátil.

La tarjeta SIM SC está diseñada para intercambiar mensajes con teléfonos de telecomunicaciones HM a través de la interfaz de comunicación IN. El teléfono de telecomunicaciones HM está diseñado para intercambiar mensajes con un servidor lejano SR mediante el mecanismo OTA. Entonces la tarjeta SIM SC puede intercambiar mensajes con el servidor lejano SR mediante la máquina anfitriona conectada HM.

El agente AA puede implementarse como un applet en Java Card. En este ejemplo las dos aplicaciones AP1 y AP2 dependen del dominio de seguridad SD. El applet AP1 comprende un medio M5 que es capaz de solicitar al agente AA el registro del applet AP1.

En una realización preferida, el agente AA puede combinarse con el Dominio de seguridad SD.

La **Figura 2** muestra un ejemplo de una primera realización de un registro RG integrado en el agente AA según la invención.

El registro RG está diseñado para contener un conjunto de pares {valor del elemento, referencia de una aplicación} . En el ejemplo de la Figura 2, el registro RG contiene dos pares: {EV1,RF1} y {EV2,RF2}.

RF1 es una referencia del applet AP1 y RF2 es una referencia del applet AP2. Por ejemplo RF1 puede ser igual a la AID del applet AP1 o una dirección específica a AP1 o a un identificador almacenado en un registro especializado.

EV1 es un valor asociado al applet AP1 y EV2 es un valor asociado al applet AP2. En esta primera realización, se supone que los valores EV1 y EV2 son los valores posibles para un campo implícito predeterminado de la cabecera del mensaje HTTP. En particular, los dos valores EV1, EV2 pueden diseñarse para ser encontrados en el campo Tipo de Contenido de la cabecera HTTP. Por ejemplo EV1 puede ser igual a "aplicación/Rastreolmei/1.0" y EV2 puede ser igual a "aplicación/PDM/1.0". En este ejemplo EV2 puede corresponderse con una aplicación de un listín telefónico en la cual PDM significa Gestor de Datos Personales.

La **Figura 3** muestra un ejemplo de una arquitectura de agente AA. El agente comprende un registro RG y cuatro medios M1, M2, M3 y M4.

El medio M1 es capaz de registrar el applet AP1. El registro es llevado a cabo mediante la asociación de una referencia RF1 de la aplicación AP1 con un valor de un elemento de la cabecera del mensaje HTTP. La referencia empleada en el registro RG permite que el agente AA identifique la aplicación a la que va dirigida para iniciarla.

Cuando un mensaje HTTP es recibido desde el servidor SR, el medio M2 es capaz de transferir parte del mensaje HTTP al applet AP1 si la cabecera del mensaje HTTP contiene un elemento igual al valor EV1 asociado a la referencia RF1. De manera similar, el medio M2 es capaz de transferir parte del mensaje HTTP recibido al applet AP2 si la cabecera del mensaje HTTP contiene un elemento igual al valor EV2 asociado a la referencia RF2. Generalmente, la parte del mensaje HTTP que es transferida al applet dirigido es el cuerpo completo del mensaje HTTP enviado por el servidor SR.

El medio M3 es capaz de comprobar si el applet AP3 cumple con las reglas de seguridad predeterminadas. El medio M3 rechaza registrar un applet si la verificación de seguridad finaliza de manera insatisfactoria. Por ejemplo el medio M3 puede verificar que el applet AP1 se encuentra en el mismo dominio de seguridad que el agente AA.

En la mayoría de los casos, el applet AP1 genera una respuesta de los datos recibidos del agente AA. El medio M4 es capaz de transferir la respuesta al servidor lejano SR. El envío de la respuesta se realiza gracias a un mensaje HTTP que contiene la respuesta.

La **Figura 4** muestra un ejemplo de una segunda realización de un registro RF integrado en el agente AA según la invención. El registro RG está diseñado para contener un conjunto de subconjuntos {Identificador del elemento de la cabecera, valor del elemento y referencia de una aplicación}. En el ejemplo de la Figura 4, el registro RG contiene un subconjunto: {HE1,EV1,RF1}. RF1 es una referencia del applet AP1 y EV1 es un valor asociado al applet AP1. HE1 es un identificador de un campo de la cabecera del mensaje HTTP. Por ejemplo, el identificador HE1 puede apuntar al campo de Tipo de Contenido. Por ejemplo HE1 puede ser igual a "Tipo de Contenido" cuando el identificador HE1 se corresponde al campo Tipo de Contenido. Alternativamente, el mensaje HTTP puede contener otra cabecera definida con campo personalizado. Por ejemplo HE1 puede ser igual a "X-Adm-Hacia" si el identificador HE1 se corresponde a una cabecera personalizada adicional del mensaje HTTP.

Según la realización de la invención, la primera etapa del método se corresponde al registro del applet AP1 en el agente AA. Por ejemplo, el registro puede ser solicitado por el propio applet AP1. El applet se encuentra registrado en el agente AA almacenando un par que comprende un valor EV1 de un elemento de la cabecera del mensaje HTTP y una referencia RF1 del applet AP1. En una realización preferida, elemento de la cabecera del mensaje HTTP es el Tipo de Contenido. El valor EV1 debe ser escogido de manera que sea diferente de los patrones definidos por los estándares OMA-SCWS y Global Platform ® 2.2.

La aplicación AP1 puede generar una solicitud de inicio de una sesión OTA. Entonces la aplicación AP1 envía esta solicitud al agente AA.

Luego el agente AA envía un primer mensaje HTTP POST al servidor remoto SR mediante la máquina anfitriona HM conectada.

Entonces el servidor remoto SR envía un mensaje de solicitud de respuesta HTTP al token SC. La cabecera de este mensaje de respuesta HTTP contiene un campo de Tipo de Contenido igual a EV1. El mensaje de respuesta HTTP es recibido por el agente AA en el token SC. El agente AA verifica si se ha registrado un applet para el valor EV1. Ya

que se ha registrado el applet AP1 y asociado al valor EV1 para el campo Tipo de Contenido, el agente AA extrae el cuerpo del mensaje de respuesta HTTP recibido. Por ejemplo, el cuerpo puede contener un comando aplicativo cuyo objetivo sea actualizar el listín telefónico. El cuerpo también puede contender un mensaje aplicativo en base a la estructura TLV o basado en otro formato relevante. Entonces el agente AA envía los datos extraídos al applet AP1. En una realización preferida, RF1 es igual a la AID del applet AP1. Entonces el agente AA es capaz de encontrar fácilmente la aplicación en cuestión. Luego el applet AP1 trata los datos recibidos y computa una respuesta correspondiente al comando aplicativo recibido. El applet AP1 envía la respuesta al agente AA. Luego el agente AA genera un mensaje HTTP POST que contiene la respuesta del applet y envía el mensaje HTTP POST al servidor SR. El applet AP1 proporciona al agente AA la URL del servidor SR. El mensaje HTTP POST se genera con una cabecera cuyo campo Tipo de Contenido está establecido en EV1 y con un cuerpo que comprende la respuesta suministrada por el applet AP1. Entonces el servidor SR recibe un mensaje HTTP POST que se corresponde al mensaje de respuesta HTTP POST inicial.

En una realización preferida tanto el servidor SR como el agente AA poseen credenciales que permite asegurar la comunicación HTTP a través de HTTPS.

Alternativamente, el registro RG puede contener un subconjunto {HE1,EV1,RF1} como se describe en la Figura 4. En especial, el identificador HE1 puede corresponderse con el campo de Tipo de Contenido de la cabecera HTTP. En este caso, el agente AA verifica si ha sido registrado un applet para el valor EV1 en el campo de la cabecera HE1.

Gracias a la invención, un servidor HTTP remoto puede enviar una transcripción completa OTA a la aplicación integrada en el token electrónico seguro. En especial, un servidor HTTP remoto puede enviar transcripciones completas OTA a una aplicación distinta de un Servidor Web de Tarjetas Con chip.

Provechosamente, cualquier intento de registro de un applet al valor de un elemento que ya está registro en otro applet será denegado.

Alternativamente, el agente AA es capaz de administrar los posibles conflictos cuando selecciona la aplicación a la que va dirigido gracias al registro RG. La regla principal es seleccionar una aplicación como máximo. O ninguna aplicación es seleccionada o se selecciona una sola aplicación conforme a una política específica predeterminada. Por ejemplo el agente AA puede seleccionar la primera aplicación que coincide con una entrada en el registro RG.

En una realización, sólo puede autorizarse un auto-registro. En otras palabras un applet puede solicitar el registro solamente para sí mismo.

Alternativamente, el registro puede delegarse en otra aplicación integrada en un token seguro SC. Entonces puede autorizarse el registro de un applet por otro applet. En este caso, el applet objetivo registrado debe ya existir en el token SC.

En otra realización, el agente AA puede también permitir el registro remoto de un applet. Entonces el servidor lejano SR puede pedir el registro del applet AP1. El agente AA puede proporcionar un comando OTA específico para el registro remoto por ejemplo. Entonces un servidor lejano puede cargar, instalar y registrar un nuevo applet en un token seguro.

Provechosamente, el agente AA puede proporcionar una característica que permita solicitar la eliminación de la entrada del applet en el registro RG. Esta característica puede implementarse gracias a un punto de entrada OTA o Java Card.

Una ventaja de la invención es permitir una administración dinámica de los canales HTTPS entre un servidor lejano y una aplicación integrada en un token seguro. Gracias al mecanismo de registro, el enlace entre la aplicación y el servidor remoto puede ser establecido y eliminado según las necesidades aplicativas y administrativas.

REIVINDICACIONES

1. Un **método** de administración de una aplicación (AP1) integrada en un token electrónico asegurado (SC), dicho token electrónico asegurado (SC) diseñado para recibir un mensaje de una máquina de servidor (SR), dicho token electrónico (SC) que comprende un agente (AA) capaz de administrar dicho mensaje, el mensaje que posee una cabecera y un cuerpo,

caracterizado porque dicho método comprende las etapas de:

(a)Registro de la aplicación (AP1) en el agente (AA) asociando una referencia (RF1) de la aplicación (AP1) con un valor de un elemento de la cabecera del mensaje,

b) cuando el mensaje es recibido desde la máquina del servidor (SR), transferir parte de dicho mensaje a la aplicación (AP1) si la cabecera del mensaje contiene un elemento que posea un valor asociado a la referencia (RF1) de la aplicación (AP1).

2. Un método según la reivindicación 1, en el que dicho método comprende la etapa adicional de:

c) cuando la aplicación (AP1) genera una respuesta al mensaje, enviar dicha respuesta a la máquina del servidor (SR).

3. Un método según reivindicación 1 y 2, en el que dicho mensaje cumple con el formato HTTP o HTTPS.

4. Un método según reivindicación 3, en el que dicha cabecera es un Tipo de Contenido como se define por el estándar HTTP-RFC 2616 HTTP/1.1.

5. Un método según una de las reivindicaciones de 1 a 4, en el que dicho agente (AA) rechaza dicha etapa de registro si la aplicación (AP1) no cumple con las reglas de seguridad predeterminadas.

6. Un método según una de las reivindicaciones de 1 a 5, en la que dicho agente (AA) rechaza la etapa de registro si el valor de dicho elemento ya está registrado en otra aplicación.

7. Un método según una de las reivindicaciones de 1 a 6, en la que dicha etapa de registro es solicitada por la aplicación (AP1).

8. Un método según una de las reivindicaciones de 1 a 6, en la cual dicho token electrónico asegurado (SC) comprende una segunda aplicación (AP2) y en la que dicha etapa de registro es solicitada por la segunda aplicación (AP2).

9. Un método según una de las reivindicaciones de 1 a 6, en la cual dicha etapa de registro es solicitada por la máquina de servidor (SR).

10. Un token electrónico asegurado (SC) diseñado para recibir un mensaje de una máquina de servidor (SR), dicho token electrónico asegurado (SC) comprende un agente (AA) capaz de administrar dicho mensaje, el mensaje que contiene una cabecera y un cuerpo, dicho token electrónico asegurado compuesto por:

- Un microprocesador (MP),

- Una interfaz de comunicación (IN),

- Un sistema operativo (OS),

- Una memoria de trabajo (MEM1) y una memoria no volátil (MEM2),

dicho token electrónico asegurado (SC) creado para comprender una aplicación (AP1),

caracterizado porque dicho agente (AA) comprende un primer y segundo medio (M1, M2), dicho primer medio siendo capaz de registrar la aplicación (AP1) mediante la asociación de una referencia (RF1) de la aplicación (AP1) con un valor de un elemento de la cabecera del mensaje y dicho segundo medio (M2) siendo capaz de transferir parte de dicho mensaje a la aplicación (AP1) si la cabecera del mensaje contiene un elemento que tenga un valor asociado a la referencia (RF1) de la aplicación (AP1).

11. Un token electrónico asegurado (SC) según la reivindicación 10, en la cual dicho agente (AA) comprende un tercer medio (M3) capaz de verificar si la aplicación (AP1) cumple con las reglas de seguridad predeterminadas y capaz de rechazar el registro de dicha aplicación (AP1) en caso de una verificación no satisfactoria.

12. Un token electrónico asegurado (SC) según una de las reivindicaciones 10 u 11, en la cual la aplicación (AP1) genera una respuesta al mensaje, y en la cual dicho agente (AA) comprende un cuarto medio (M49) capaz de transferir dicha respuesta a la máquina de servidor (SR).

13. Un token electrónico asegurado (SC) según una de las reivindicaciones de 10 a 12, en la cual la aplicación (AP1) comprende un quinto medio (M5) capaz de solicitar al agente (AA) el registro de la aplicación (AP1).

14. Un token electrónico asegurado (SC) según una de las reivindicaciones de 10 a 13, en la cual dicho mensaje cumple con el formato HTTP o HTTPS y en la cual dicho elemento de cabecera es un Tipo de Contenido como se define por el estándar HTTP-RFC 2616 HTTP/1.1.

15. Un token electrónico asegurado (SC) según una de las reivindicaciones 10 A 14, en la que dicho token electrónico asegurado (SC) es una tarjeta con chip.

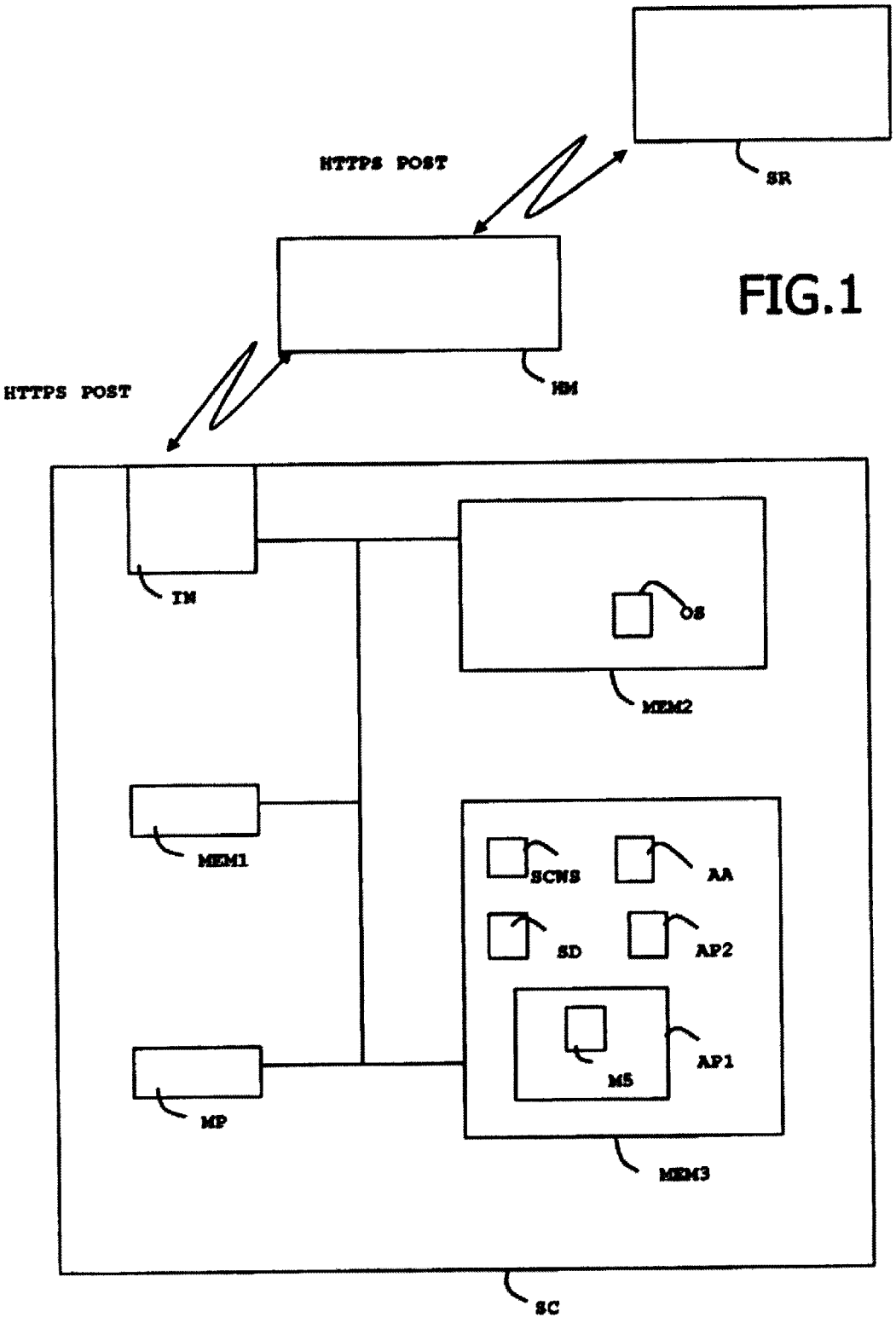
HTTPS POST
SR
HTTPS POST
HM
IN
OS
MEM2
MEM1
SCWS
AA
SD
AP2
M5
AP1
MP
MEM3
SC

FIG.1

FIG.2

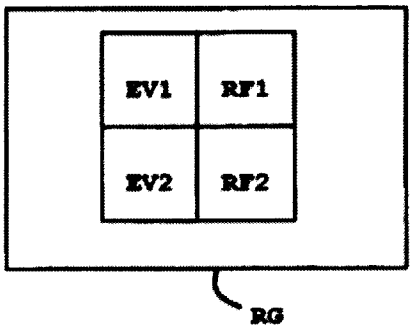

FIG.3

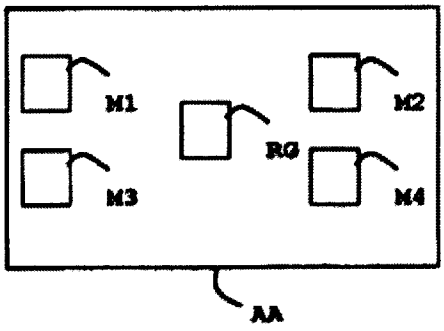

FIG.4