(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 531 250**

(51) Int. CI.:

G06F 21/00 (2013.01)
H04L 29/06 (2006.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.10.2011 E 11775991 (0)**

(97) Fecha y número de publicación de la concesión europea: **24.09.2014 EP 2641206**

(54) Título: **Método de carga de datos de un token seguro portátil**

(30) Prioridad:

15.11.2010 EP 10306254

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.03.2015

(73) Titular/es:

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

(72) Inventor/es:

AMIEL, PATRICE;
BERARD, XAVIER;
PREULIER, ERIC y
GALLAS, FREDERIC

(74) Agente/Representante:

ISERN CUYAS, María Luisa

DESCRIPCIÓN

Método de carga de datos en un token seguro portátil.

La presente invención se refiere a los métodos de carga de datos en tokens seguros portátiles. Se refiere particularmente a los métodos de carga de datos en tokens seguros portátiles que contienen una pluralidad de entidades destinadas a obtener datos gracias a los mecanismos de votación. En particular, dichos tokens seguros portátiles pueden ser tarjetas SIM.

(Estado de la Técnica anterior)

Los tokens seguros portátiles son pequeñas máquinas que comprenden una memoria, un microprocesador y un sistema operativo para el cálculo de los tratamientos. Los tokens seguros portátiles están destinados a conectar - ya sea en el modo de contacto o sin contacto - una máquina anfitriona que puede proporciona energía y una interfaz de usuario. En general, los tokens seguros portátiles comprenden una pluralidad de memorias de diferentes tipos. Por ejemplo, pueden comprender memoria RAM, ROM, EEPROM o tipo Flash. Los tokens portátiles tienen recursos informáticos limitados. Por ejemplo, las tarjetas inteligentes son tokens electrónicos seguros.

En el dominio Telecom, una tarjeta de circuito integrado universal (UICC) está conectada a un teléfono móvil. Por lo general, la UICC sondea un servidor distante para saber si hay algo de contenido para ser entregado a la UICC. Por ejemplo, la UICC puede sondear un servidor remoto utilizando el mecanismo de Over-The-Air (OTA) a lo largo de un protocolo de transferencia de hipertexto (HTTP) ó un protocolo seguro de transferencia de hipertexto (HTTPS). La UICC puede incrustar una o varias aplicaciones que necesita para sondear uno o varios servidores de aplicaciones distantes. Cuando una aplicación sondea el servidor remoto, la mayoría de las veces, no hay datos para recuperar por la aplicación. Un problema es que dicho mecanismo de sondeo genera una gran cantidad de las comunicaciones inútiles entre cada UICC y el servidor distante. Un mensaje de sondeo inútil significa que el mensaje de sondeo no conduce a una carga de datos en el token seguro. Cuando sólo una entidad está en modo de sondeo, es fácil de configurar el período de sondeo para hacer que el número de comunicaciones inútiles sea aceptable. Sin embargo, es mucho más complejo evaluar el comportamiento general cuando varias entidades están solicitando sesiones para comunicar con los servidores remotos.

Por otra parte una UICC puede comprender varios dominios de seguridad según la definición de las especificaciones de la Plataforma Global de la tarjeta inteligente V2.2 y Enmienda B. Un dominio de seguridad comprende un Agente Admon. (también llamado agente de administración) que es capaz de gestionar su propio mecanismo de sondeo. Cuando una pluralidad de aplicaciones pertenecen a diferentes dominios de seguridad, el número de mensajes de sondeo enviados por un UICC no puede ser optimizado ya que cada Agente Admon. trabaja de forma independiente.

Se conoce el uso de una aplicación especifica que está incrustado en un token seguro. Esta aplicación específica permite gestionar políticas de sondeo automáticas basadas en el tiempo o en un evento preestablecido. En consecuencia, es posible optimizar el sondeo de un dominio de seguridad. Desafortunadamente, esta solución se limita a las aplicaciones que pertenecen a un mismo dominio de seguridad para sondeo.

Se sabe cómo maximizar la duración entre dos solicitudes de sondeo de manera que el sondeo global realizado por la UICC sea limitado. Esta solución no es, con frecuencia, compatible con los requerimientos del negocio, porque la mayoría de las aplicaciones necesitan actualizaciones periódicas.

El mecanismo de sondeo se basa en el principio de la extracción. En un mecanismo de extracción, la UICC toma la iniciativa de solicitar los datos a un servidor distante. Otra solución conocida consiste en utilizar un mecanismo de empuje en vez de un mecanismo de extracción. En el mecanismo de empuje, el servidor distante toma la iniciativa en el envío de datos a una aplicación de la UICC. Por desgracia, el mecanismo de empuje presenta muchos inconvenientes con respecto a la parte del servidor y el consumo de la red.

Hay una necesidad de proporcionar una solución para optimizar el modo de sondeo para una pluralidad de componentes unidos a diferentes dominios de seguridad.

(Resumen de la invención)

Un objeto de la invención es resolver el problema técnico antes mencionado. La invención permite reducir el número de mensajes intercambiados entre un token seguro portátil que comprende varias aplicaciones y los servidores de aplicaciones correspondientes a estas aplicaciones. La invención se basa en un agente admon. que sondea un determinado servidor de administración - llamado servidor sindicación - y recibe una lista de acciones a realizar por al menos otro agente admon. del token seguro portátil. Así, el número de agentes admon. que periódicamente sondean los servidores de aplicaciones pueden reducirse para un token de seguridad portátil. Los servidores de aplicaciones correspondientes se supone que declaran una lista de operaciones dirigidas al token seguro portátil para el servidor de sindicación.

El objeto de la presente invención es un método para cargar datos en un token seguro portátil. El token seguro comprende una pluralidad de dominios de seguridad. Un primer dominio de seguridad comprende un primer agente de administración y un segundo dominio de seguridad comprende un segundo agente de administración. Un servidor de aplicaciones remoto comprende proporcionar unos primeros datos al segundo agente de administración. Una lista es enviada en respuesta a una solicitud de sondeo. Esta lista incluye una referencia a los primeros datos. Un servidor de sindicación contiene la lista. La solicitud de sondeo es enviada por el primer agente de administración. La lista está comprendida en una respuesta de sondeo enviada por el servidor sindicación. El servidor de sindicación es distinto del servidor de aplicaciones remoto.

Ventajosamente, el método puede comprender los pasos de enviar la lista desde el primer agente de administración al segundo agente de administración, y de recuperar dichos datos por parte del segundo agente de administración del servidor de aplicaciones remoto, mediante el uso de la lista.

Ventajosamente, la solicitud de sondeo puede ser enviada a través de un primer protocolo de comunicación y dichos primeros datos pueden ser cargados en el token seguro a través de un segundo protocolo de comunicación que tiene características de seguridad superiores al primer protocolo de comunicación.

En una realización, el primer protocolo de comunicación puede ser HTTP y dicho segundo protocolo de comunicación puede ser HTTPS.

Ventajosamente, la lista puede ser actualizada en el servidor de sindicación después de los primeros datos se hayan cargado en el token seguro.

En una realización, dicho servidor de sindicación puede comprender una segunda lista dirigida a dicho primer agente de administración. La segunda lista puede comprender una referencia a los segundos datos que se almacenan en un segundo servidor de aplicaciones remoto. La respuesta de sondeo puede comprender la segunda lista.

Ventajosamente, el segundo dominio de seguridad puede comprender una aplicación y dichos primeros datos pueden ser proporcionados a dicha aplicación por el segundo agente de administración.

Otro objeto de la invención es un token seguro portátil que comprende una pluralidad de dominios de seguridad en el que un primer dominio de seguridad comprende un primer agente de administración, y en el que un segundo dominio de seguridad comprende un segundo agente de administración. El primer agente de administración está adaptado para enviar una solicitud de sondeo a un servidor preestablecido y recibir una respuesta de sondeo. El segundo agente de administración tiene como objetivo obtener unos primeros datos de un servidor de aplicaciones remoto. El servidor predeterminado es un servidor de sindicación distinto del servidor de aplicaciones remoto. El primer dominio de seguridad comprende primeros y segundos recursos.
Los primeros recursos están adaptados para identificar una lista que comprende una referencia a los primeros datos en dicha respuesta de sondeo. Los segundos recursos están adaptados para enviar la lista al segundo agente de administración.

Ventajosamente, dicho primer agente de administración puede ser adaptado para enviar la petición de sondeo a través de un primer protocolo de comunicación y dicho segundo agente de administración puede ser adaptado para cargar los primeros datos en el token seguro a través de un segundo protocolo de comunicación que tiene características de seguridad superiores al primer protocolo de comunicación.

En una realización, dicho primer protocolo de comunicación puede ser HTTP y dicho segundo protocolo de comunicación puede ser HTTPS.

(Breve descripción de los dibujos)

Otras características y ventajas de la presente invención emergerán más claramente de la lectura de la siguiente descripción de un número de realizaciones preferidas de la invención con referencia a los correspondientes dibujos que acompañan, en los que:

- La figura 1 representa esquemáticamente un ejemplo de un sistema que comprende una pluralidad de servidores de aplicaciones, un servidor de sindicación y un token seguro portátil de acuerdo con la invención;

- La figura 2 representa esquemáticamente otro ejemplo de un sistema que comprende una pluralidad de servidores de aplicaciones, dos servidores de sindicación y un token seguro portátil de acuerdo con la invención; y

- La figura 3 representa esquemáticamente un ejemplo de un dominio de seguridad que comprende un agente admon. de acuerdo con la invención.

(Descripción detallada de las realizaciones preferidas)

La invención puede aplicarse a cualquier tipo de token seguro portátil que comprenden varios agentes admon. capaces de establecer una sesión de comunicación con servidores de aplicaciones distantes.

La Figura 1 muestra un ejemplo de un sistema SY que comprende un servidor de sindicación SS, un token portátil seguro SC y cuatro servidores de aplicaciones AS1, AS2, AS3 y AS4. La figura 1 también muestra un ejemplo de un método de acuerdo con la invención.

En el ejemplo de la Figura 1, el token portátil seguro SC es una UICC que comprende tres dominios de seguridad SD1, SD2 y SD3. El dominio de seguridad SD1 contiene un agente admon. AA1 y una aplicación AP11. El agente admon. AA1 es un componente que es capaz de gestionar una OTA a través de conexión HTTP entre el dominio de seguridad SD1 y un servidor distante. El dominio de seguridad DS2 contiene un agente admon. AA2. El dominio de seguridad SD3 contiene un agente admon. AA3 y una aplicación AP31.

El servidor de aplicaciones AS1 es un servidor remoto que comprende unos datos D1 destinados a ser enviados a la aplicación AP11. El servidor de aplicaciones AS3 es un servidor remoto que comprende unos datos D3 destinados a ser enviados a la aplicación AP31.

De acuerdo con una primera realización del método de la invención, los servidores de aplicaciones AS1 y AS3 declaran sus respectivos datos D1 y D3 al servidor de sindicación SS en el paso ST1. Durante el paso ST1, dos listas L1 y L3 se registran en el servidor de sindicación SS. La lista L1 contiene una referencia a los datos D1, un identificador de aplicación AP11 y un identificador del token SC. La lista L3 contiene una referencia a los datos D3, un identificador de aplicación AP31 y un identificador del token SC.

La referencia a los datos D1, respectivamente D3, puede contener un Identificador Uniforme de Recursos (URI) del servidor de aplicación AS1, respectivamente AS3.

Ventajosamente, la lista L1 respectivamente, la lista L3 puede contener un identificador de un conjunto de varias tokens seguros portátiles en lugar del identificador del token SC. Esta última realización permite la orientación de una colección de tokens con los mismos datos almacenados en un servidor de aplicaciones.

Ventajosamente, la lista L1 respectivamente, la lista L3 puede contener un identificador del agente admon. AA1, respectivamente AA3.

En una realización la lista L3 se envía directamente desde el servidor de aplicaciones AS3 al servidor de sindicación SS. Ventajosamente, el envío de la lista L3 puede estar protegida por las pertinentes características de seguridad a fin de garantizar la confidencialidad y la integridad de la lista enviada. Dichas características de seguridad son bien conocidas para una persona experta en la técnica.

Al final de la etapa ST1, tanto la lista L1 como la L3 se almacenan en el servidor de sindicación SS. Obviamente, en otras realizaciones del método, cualquier número de lista se puede almacenar en el servidor de sindicación SS durante el paso ST1. Por ejemplo, al final de la etapa ST1, el servidor SS puede contener uno, tres o diez listas. Alternativamente, el servidor SS también puede no contener lista alguna si no hay datos para ser cargados en el token de seguridad portátil.

A continuación en la etapa ST2, se envía una solicitud de sondeo desde el token SC al servidor de sindicación SS. La solicitud de sondeo es gestionada por el agente admon. AA1. En la realización de la Figura 1, un mecanismo de sondeo está activo sólo en el agente admon. AA1. En otras palabras, ni el agente admon. AA2 ni el agente admon. AA3 envían ningún mensaje de sondeo. En una realización preferida, la solicitud de sondeo contiene un identificador del token seguro contador SC.

En el paso ST3, el servidor sindicación SS comprueba si contiene una lista focalizando el token seguro SC. El identificador extraído de la solicitud de sondeo recibida puede ser utilizado para la identificación de la lista pertinente. En el ejemplo de la Figura 1, las listas L1 y L3 son encontradas como dirigidas al token seguro SC. En otras palabras, los componentes de focalización de las listas L1 y L3 están incrustados en el token seguro SC.

En respuesta a la solicitud de sondeo recibida, el servidor de sindicación SS construye una respuesta de sondeo que contiene las dos listas identificadas L1 y L3. El servidor de sindicación SS envía la respuesta de sondeo para el agente admon. AA1 en el paso ST4. Se recibe la respuesta de sondeo y es analizada por agente admon. AA1. Al revisar el contenido de las listas L1 y L3, el agente admon. AA1 identifica la lista L1 como destinada a la aplicación AP11 y la lista L3 como destinada a la aplicación AP31. En particular, el agente admon. AA1 puede utilizar el identificador de aplicación contenida en cada lista recibida.

Luego en el paso ST5, el agente admon. AA1 envía la lista L3 al agente admon. AA3 que se encarga de gestionar la aplicación AP31. La lista L3 contiene el identificador de la aplicación AP31. El sistema operativo del token seguro SC

es capaz de identificar el dominio de seguridad SD3 que contiene la aplicación AP31. Entonces el agente admon. AA3 que pertenece al dominio de seguridad identificado SD3 es identificado como el agente admon. a cargo de la aplicación AP31.

En la etapa ST6, el agente admon. AA1 abre una sesión de comunicación con el servidor de aplicaciones distante AS1 con el fin de obtener los datos D1. Esta sesión de comunicación se puede realizar a través de OTA, a través de HTTP o de cualquier canal de comunicación relevante. Entonces el agente admon. AA1 recibe los datos D1 y proporciona los datos D1 a la aplicación AP11.

En el paso ST7, el agente admon. AA3 abre una sesión de comunicación con el servidor de aplicaciones distante AS3 con el fin de obtener los datos D3. La lista L3 contiene datos de conectividad que permite al agente admon. AA3 acceder al servidor de aplicaciones relevantes AS3. Por ejemplo los datos de conectividad pueden ser el URL (Uniform Resource Locator) del servidor AS3. Los datos de conectividad también pueden contener datos relativos a los parámetros de seguridad del nivel de seguridad para ser utilizados para acceder al servidor de aplicaciones.

Ventajosamente, el agente admon. AA3 puede ser capaz de ponerse en contacto automáticamente con una URL preestablecida. Por ejemplo, el agente admon. AA3 puede tener acceso a un parámetro predefinido que contiene la dirección URL del servidor AS3.

Esta sesión de comunicación se puede realizar a través de una OTA, a través de HTTPS o de cualquier canal de comunicación pertinente. Entonces el agente admon. AA3 recibe los datos D3 y le proporciona dichos datos D3 a la aplicación AP31. Los datos D3 pueden contener una versión actualizada de la aplicación AP31, datos aplicativos para ser utilizado por la aplicación AP31 ó datos de seguridad (como una clave secreta) para ser utilizados por la aplicación AP31. Los datos D3 también pueden contener un comando o un parámetro aplicativo.

Ventajosamente, se proporciona una retroinformación al servidor de sindicación SS cuando los datos se envían por un servidor de aplicaciones al token seguro SC. Una retroinformación de este tipo permite evitar un mayor envío de los mismos datos para el token seguro SC. Dicha retroinformación podrá enviarse bien por el servidor de aplicaciones o por el token seguro SC.

En otra realización, el servidor de sindicación SS puede contener sólo la lista L3. Por lo tanto, en respuesta a una solicitud de sondeo, el agente admon. AA1 recibe una respuesta de sondeo que contiene sólo la lista L3. En tal caso, el agente admon. AA1 analiza la respuesta de sondeo recibida y envía la lista L3 al agente admon. AA3. El agente admon. AA1 no envía ningún dato a la aplicación que pertenece a su dominio de seguridad SD1. El agente admon. AA1 permanece a cargo de su mecanismo de sondeo y enviará otra solicitud de sondeo al servidor de sindicación SS.

En la realización de la figura 1, los agentes de administración AA2 y AA3 no manejan ningún mecanismo de sondeo.

Ventajosamente, sólo el agente admon. AA1 tiene una política de sondeo.

En una realización preferida, el agente admon. AA1 pertenece al Dominio Emisor de Seguridad (ISD) tal como se define en el estándar de la Plataforma Global de Especificaciones de Tarjetas V2.2.

Es de señalar que cada agente admon. Del token seguro portátil SC también puede tener su propio mecanismo de sondeo en paralelo al método de sondeo de la invención. Así, el método de la invención es compatible con un token seguro que comprende un agente admon. que debe mantener su propio mecanismo de sondeo.

En una realización, el protocolo utilizado para los mensajes de sondeo es HTTP. Por ejemplo, las solicitudes de sondeo se pueden realizar a través de mensajes "post HTTP" y las respuestas de sondeo se pueden realizar a través de mensajes de "post respuesta HTTP". Las respuestas de sondeo pueden contener un contenido/tipo específico dedicado para la invención. Este nuevo contenido/tipo específico permite que el agente admon. destinatario sepa cómo analizar el mensaje recibido.

Por ejemplo, puede ser enviado el siguiente "mensaje POST":

"POST/servidor/Servidor sindicación HTTP/1.1 CRLF
Alojamiento: 172.96.0.1 CRLF
Agente-Usuario: sindicación/1.0 CRLF
CRLF "

En respuesta, puede ser enviado el siguiente "mensaje de respuesta POST":

"HTTP/1.1 200 OK CRLF
Agente-Usuario: sindicación/1.0 CRLF
Contenido-Tipo: aplicación/vnd.tarjeta-sindicación /1.0 CRLF

Contenido-Longitud: xxxx CRLF
CRLF
[L1]
[L3] "
Donde "xxxx" representa el número de bytes de los datos transmitidos.

En una realización, los mensajes de sondeo pueden ser enviados a través de un primer tipo de canal de comunicación y los mensajes intercambiados entre los servidores de aplicaciones y los agentes de administración pueden ser enviados a través de un segundo tipo de canal de comunicación.

Ventajosamente, el primer tipo de canal de comunicación puede tener un nivel de seguridad ligero ya que no se intercambian datos críticos a través de este canal. Por otro lado, el segundo tipo de canal de comunicación puede tener un nivel de seguridad alto. Por ejemplo, el primer tipo de canal de comunicación puede ser HTTP y el segundo tipo de canal de comunicación puede ser HTTPS. Gracias a esta realización particular, el tiempo y ancho de banda de los recursos se puede guardar en el tratamiento de los mensajes de sondeo porque el establecimiento de una sesión de HTTP requiere menos recursos y tiempo que el establecimiento de una sesión HTTPS.

Por lo tanto si no hay datos se que recuperar del servidor de aplicaciones, no se establece una conexión HTTPS.

La Figura 2 proporciona un segundo ejemplo de un sistema que comprende dos servidores de sindicación SS1 y SS2, SC2 un token portátil seguro y seis servidores de aplicaciones AS5 a AS10.

En el ejemplo de la Figura 2, el token seguro portátil SC2 es una tarjeta SIM que comprende tres dominios de seguridad SD4, SD5 y SD6. El dominio de seguridad SD4 contiene un agente admon. AA4 y dos aplicaciones AP41 y AP42. El dominio de seguridad SD5 contiene un agente admon. AA5 y una aplicación AP51. El dominio de seguridad SD6 contiene un agente admon. AA6 y dos aplicaciones AP61 y AP62.

El servidor de sindicación SS1 comprende dos listas L4 y L5 que se focalizan en, respectivamente, las aplicaciones AP42 y AP51. Cada una de las listas de L4 y L5 contiene una referencia a los datos almacenados en los servidores de aplicaciones AS5 a AS7. De acuerdo con una realización de la invención, el agente admon. AA4 es el encargado de gestionar un mecanismo de sondeo para los dominios de seguridad tanto SD4 como SD5.

El servidor de sindicación SS2 comprende una lista L6 que se focaliza en la aplicación AP62. La lista L6 contiene una referencia a los datos almacenados en uno de los servidores de aplicaciones AS8 a AS10. De acuerdo con una realización de la invención, el agente admon. AA6 es el encargado de gestionar un mecanismo de sondeo solamente para el dominio de seguridad SD6. Así, los dos mecanismos de sondeo pueden ser manejados de manera simultánea en el token SC2. Esta realización puede ser relevante para la gestión de la comunicación con varios grupos de servidores de aplicaciones. En el ejemplo de la Figura 2, los servidores de aplicaciones AS5, AS6 y AS7 pertenecer a un primer grupo, mientras que los servidores de aplicaciones AS8, AS9 y AS10 pertenecen a un segundo grupo.

El agente admon. AA4 está a cargo de la gestión de sondeo para el grupo (AS5, AS6 y AS7) vinculado al servidor de sindicación SS1.

Por ejemplo, el agente admon. AA4 puede enviar una solicitud de sondeo RE1 al servidor de sindicación SS1. En respuesta a RE1, el servidor SS1 puede enviar una respuesta de sondeo AN1 que contiene dos listas L4 y L5. Suponiendo que la lista L5 se dirige a un componente perteneciente al dominio de seguridad SD5, la lista L5 se envía desde el agente admon. AA4 para el agente admon. AA5. A continuación, la lista L5 se utiliza para la recuperación de datos en el servidor de aplicaciones relevantes pertenecientes al grupo vinculado al servidor de sindicación SS1.

El agente admon. AA6 está a cargo de la gestión de sondeo para el grupo (AS8, AS9 y AS10) vinculado al servidor de sindicación SS2.

El agente admon. AA6 puede enviar una solicitud de sondeo RE2 al servidor de sindicación SS2. En respuesta a RE2, el servidor SS2 puede enviar una respuesta de sondeo AN2 que contiene la lista L6. Suponiendo que la lista L6 se dirige a un componente perteneciente al dominio de seguridad SD6, la lista L6 se utiliza para la recuperación de datos en el servidor de aplicaciones relevantes que pertenecen al grupo vinculado al servidor de sindicación SS2.

La Figura 3 proporciona un ejemplo detallado del dominio de seguridad SD1 de la Figura 1.

El dominio de seguridad SD1 comprende un agente admon. AA1 y una aplicación AP11 destinada a recibir los datos de un servidor de aplicaciones distante AS1.

El agente admon. AA1 está compuesto por cuatro medios M1, M2, M3 y M4. El medio M1 está adaptado para analizar el contenido de las respuestas de sondeo y la identificación de los agente admon. que son focalizados por

este contenido. El medio M1 es capaz de extraer los datos que se han de enviar a cada agente admon. focalizado.

El medio M2 está adaptado para enviar los datos pertinentes a cada agente admon. focalizado. En otras palabras, el medio M2 es capaz de notificar a cada agente admon. focalizado del token seguro la lista de datos para ser recuperados del lado servidor de aplicaciones. El medio M2 también está adaptado para enviar los datos pertinentes para la aplicación específica que pertenece al dominio de seguridad SD1. Tal envío de datos puede implementarse a través de mecanismos que son bien conocidos por una persona experta en la técnica. Por ejemplo, un mecanismo de este tipo se utiliza para el envío de datos para la Gestión de Aplicaciones Remotas (RAM) a través de HTTP.

El medio M3 está adaptado para establecer un canal de comunicación CH1 con el servidor de sindicación SS. Este canal CH1 se establece a través de un ordenador central (no mostrado en la Figura 3) conectado al token SC. El medio M3 está adaptado para enviar y recibir mensajes de sondeo a través del canal de comunicación CH1. En una realización, el canal de comunicación CH1 es OTA a través de HTTP.

El medio M4 está adaptados para establecer un canal de comunicación CH2 con el servidor de aplicaciones AS1. Este canal CH2 se establece a través de un ordenador central (no mostrado en la figura 3) conectado al token SC. El medio M4 está adaptado para enviar y recibir mensajes con el fin de recuperar los datos D1 a través del canal de comunicación CH2 de una manera segura. En una realización, el canal de comunicación CH2 es OTA a través de HTTPS.

Los cuatro medios M1 a M4 han sido descritos como cuatro componentes distintos. Ellos pueden implementarse como uno o varios componentes.

En las realizaciones descritas anteriormente, el token seguro portátil SC es una UICC o una tarjeta SIM. Tales tokens comprenden un sistema operativo OS, una memoria de trabajo, un microprocesador, una memoria no volátil y una interfaz de comunicación para comunicar con una máquina huésped. La invención también se aplica a los tokens como tarjetas inteligentes con o sin contacto, tokens USB, tokens NFC, etc.

Gracias a la invención, un mecanismo de sondeo que es común a una pluralidad de agente admon. es manejado por un solo agente admon. El agente admon., a cargo de gestión de sondeo, sondea el servidor de sindicación con el fin de saber si al menos un agente admon. de la pluralidad de agente admon. debe recuperar datos de un servidor de aplicaciones. La sindicación envía una lista de actividades a realizar en el token seguro portátil. Cada elemento de la lista se notifica al agente admon. focalizado. Cada agente admon. focalizado establece una sesión de comunicación con el servidor de aplicaciones correspondiente a fin de obtener los datos a transferir. En comparación con los modos de sondeo habituales en tokens de la técnica anterior, la invención permite evitar un gran número de mensajes de sondeo que no conducen a una transferencia de datos entre un servidor de aplicaciones y el token seguro portátil.

Los datos recuperados por el token SC de un servidor de aplicaciones puede ser una actualización de un componente ejecutable de una aplicación integrada en el token, parámetros de seguridad o parámetros aplicativos relacionados con una aplicación incorporada en el token seguro.

Una ventaja de la invención es permitir el ahorro de ancho de banda OTA cuando un gran número de tarjetas UICC o SIM se implementa en el campo. En particular, la invención permite optimizar el mecanismo de sondeo para la Gestión de Aplicaciones Remotas (RAM) a través de HTTP/HTTPS, Gestión de Aplicaciones Remotas (RFM) a través de HTTP/HTTPS y Servidor Web de Tarjeta Inteligente (SCWS) a través de HTTP/HTTPS. La invención permite el ahorro de recursos de red móvil de operadores de redes móviles (MNO).

Aunque las realizaciones descritas anteriormente están orientados sobre la OTA a través de HTTP o HTTPS, la invención también se aplica a cualquier tipo de canal de comunicación en el que la conexión se realiza por iniciativa token. Por ejemplo, la invención se aplica al canal de comunicación de HTTP a través del tipo TCP/IP. La invención también se aplica a canal de comunicación de CAT-TP (Protocolo de Transporte de Aplicación de Tarjeta) a través de UDP (Protocolo de Usuario Datagram) o cualquier protocolo utilizado sobre un canal BIP (Protocolo de Portador Independiente).

REIVINDICACIONES

1. Un método en un sistema que comprende un token seguro portátil (SC) y un servidor de aplicaciones remoto (AS3), comprendiendo dicho token seguro portátil (SC) una pluralidad de dominios de seguridad (SD1, SD2) en el que el primer dominio de seguridad (SD1) comprende un primer agente de administración (AA1), y en el que un segundo dominio de seguridad (SD3) comprende un segundo agente de administración (AA3), comprendiendo el servidor de aplicaciones remoto (AS3) unos primeros datos (D3) para ser proporcionados al segundo agente de administración (AA3), siendo enviada una lista (L3) en respuesta a una solicitud de sondeo, comprendiendo dicha lista (L3) una referencia a los primeros datos (D3),
caracterizado porque el sistema comprende un servidor de sindicación (SS) que contiene dicha lista (L3), **y porque** la solicitud de sondeo es enviada por el primer agente de administración (AA1) **y porque** la lista (L3) está comprendida en una respuesta de sondeo enviada por el servidor de sindicación (SS), siendo dicho servidor de sindicación (SS) distinto del servidor de aplicaciones remoto (AS3).

2. Un método de acuerdo con la reivindicación 1, en el que dicho método comprende las etapas de:

- enviar dicha lista (L3) del primer agente de administración (AA1) al segundo agente administración (AA3),
- recuperar dichos datos (D3) por parte del segundo agente de administración (AA3) del servidor de aplicaciones remoto (AS3), mediante el uso de la lista (L3).

3. Un método de acuerdo con una cualquiera de las reivindicaciones 1 a 2, en el que dicha lista (L3) se actualiza en el servidor de sindicación (SS) después de que los primeros datos (D3) hayan sido cargados en el token de seguridad (SC).

4. Un método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que dicho servidor de sindicación (SS) comprende una segunda lista (L1) que focaliza dicho primer agente de administración (AA1), en el que la segunda lista (L1) comprende una referencia a unos segundos datos (D1) que se almacena en un segundo servidor de aplicaciones remoto (AS1) y en el que dicha respuesta de sondeo comprende la segunda lista (L1).

5. Un método de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en el que el segundo dominio de seguridad (SD3) comprende una aplicación (AP31) y en el que dichos primeros datos (D3) son proporcionados a la aplicación (AP31) por el segundo agente de administración (AA3).

6. Un método de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en el que la solicitud de sondeo se envía a través de un primer protocolo de comunicación y en el que dichos primeros datos (D3) se cargan en el token seguro (SC) a través de un segundo protocolo de comunicación que tiene características de seguridad superiores al primer protocolo de comunicación.

7. Un método de acuerdo con la reivindicación 6, en el que dicho primer protocolo de comunicación es HTTP y dicho segundo protocolo de comunicación es HTTPS.

8. Un **token seguro portátil** (SC) diseñado para comunicar con un sistema que comprende un servidor de aplicaciones remoto (AS3) y un servidor predeterminado (SS), comprendiendo dicho token seguro portátil (SC) una pluralidad de dominios de seguridad (SD1, SD2) en el que un primer dominio de seguridad (SD1) comprende un primer agente de administración (AA1), y en el que un segundo dominio de seguridad (SD3) comprende un segundo agente de administración (AA3), estando adaptado dicho primer agente de administración (AA1) para enviar una solicitud de sondeo a un servidor predeterminado (SS) y para recibir una respuesta de sondeo, estando pensado dicho segundo agente de administración (AA3) para obtener unos primeros datos (D3) del servidor de aplicaciones remoto (AS3),
caracterizado porque el servidor predeterminado (SS) es un servidor de sindicación (SS) distinto del servidor de aplicaciones remoto (AS3), **porque** el primer dominio de seguridad (SD1) comprende unos primeros y segundos medios (M1, M2), estando adaptados dichos primeros medios (M1) para identificar una lista (L3) que comprende una referencia a los primeros datos (D3) en dicha respuesta de sondeo y dichos segundos medios (M2) estando adaptados para enviar la lista (L3) al segundo agente de administración (AA3).

9. Un token seguro portátil (SC) de acuerdo con la reivindicación 8, en el que dicho primer agente de administración (AA1) está adaptado para enviar la petición de sondeo a través de un primer protocolo de comunicación y en el que dicho segundo agente de administración (AA3) está adaptado para cargar los primeros datos (D3) en el token seguro (SC) a través de un segundo protocolo de comunicación que tiene características de seguridad superiores al primer protocolo de comunicación.

10. Un token portátil seguro (SC) de acuerdo con la reivindicación 9, en el que dicho primer protocolo de comunicación es HTTP y dicho segundo protocolo de comunicación es HTTPS.

11. Un sistema que comprende un token seguro portátil (SC) y un servidor de aplicaciones remoto (AS3),

comprendiendo dicho token seguro portátil (SC) comprende una pluralidad de dominios de seguridad (SD1, SD2) en el que el primer dominio de seguridad (SD1) comprende un primer agente de administración (AA1), y en el que un segundo dominio de seguridad (SD3) comprende un segundo agente de administración (AA3), comprendiendo el servidor de aplicaciones remoto (AS3) unos primeros datos (D3) para ser proporcionados al segundo agente de administración (AA3), siendo enviada una lista (L3) en respuesta a una solicitud de sondeo, comprendiendo dicha lista (L3) una referencia a los primeros datos (D3),
caracterizado porque el sistema comprende un servidor de sindicación (SS) que contiene dicha lista (L3), **y porque** el primer agente de administración (AA1) está adaptado para enviar la solicitud de sondeo al servidor de sindicación (SS), **y porque** el servidor de sindicación (SS) está adaptado para enviar una respuesta de sondeo que comprende la lista (L3), **y porque** dicho servidor de sindicación (SS) es distinto del servidor de aplicaciones remoto (AS3).

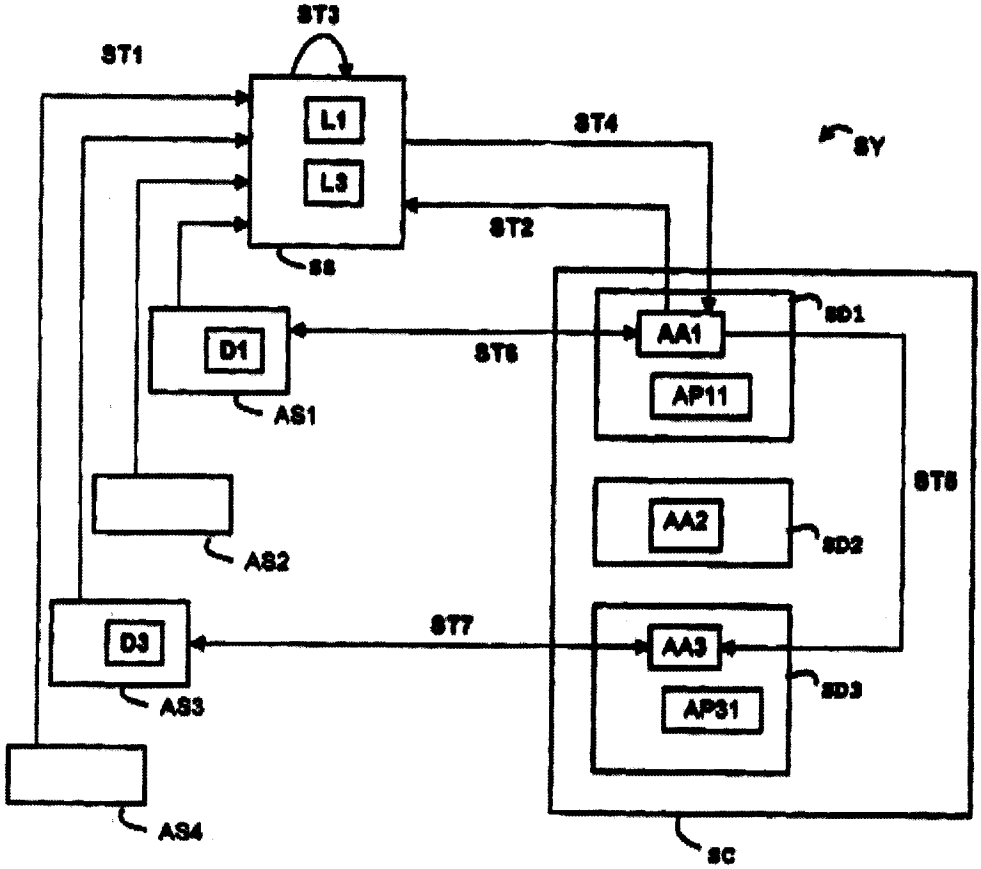
ST3
ST1
L1
L3
ST4
SY
ST2
SS
D1
AS1
AA1
SD1
AP11
ST6
ST5
AA2
SD2
AS2
D3
ST7
AA3
SD3
AP31
AS3
AS4
SC

FIG.1

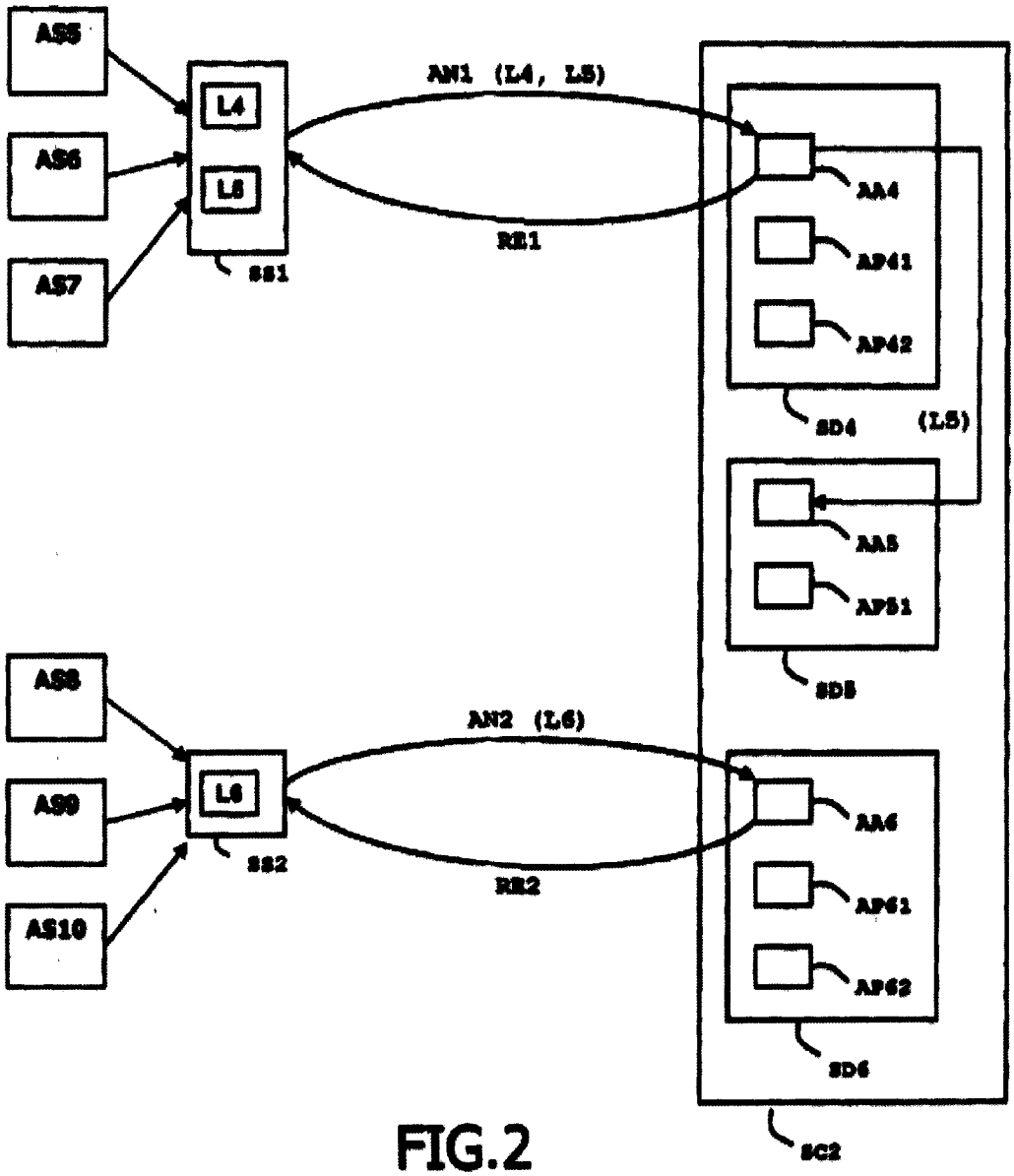
AS5
AS6
AS7
L4
L5
SS1
AN1 (L4, L5)
RR1
AA4
AP41
AP42
SD4
(L5)
AA5
AP51
SD5
AS8
AS9
AS10
L6
SS2
AN2 (L6)
RR2
AA6
AP61
AP62
SD6
SC2

FIG.2

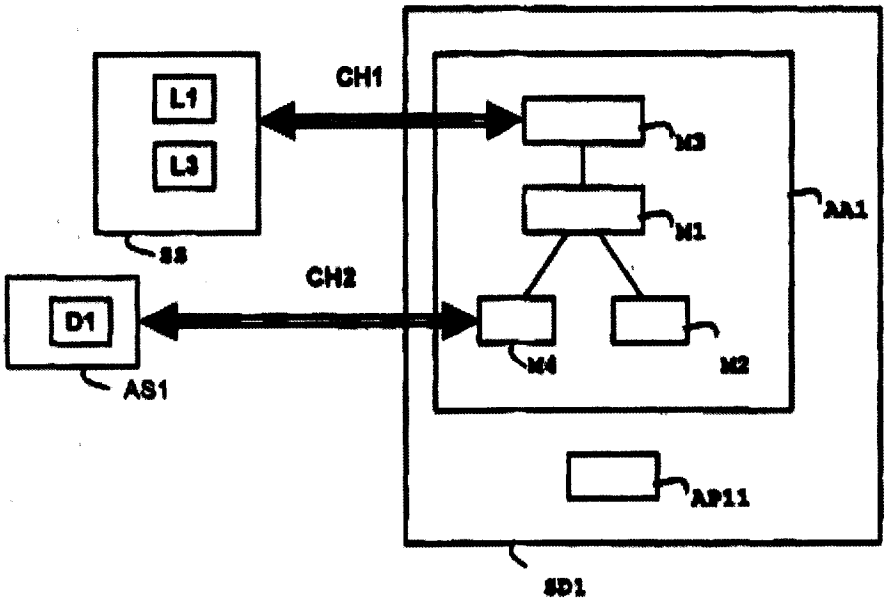

FIG.3