(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 831 384**

(51) Int. CI.:

***H04W 4/50*** (2008.01)
***H04W 12/02*** (2009.01)
***H04W 12/00*** (2009.01)
*H04W 8/18* (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.09.2014 PCT/EP2014/069152**

(87) Fecha y número de publicación internacional: **26.03.2015 WO15039923**

(96) Fecha de presentación y número de la solicitud europea: **09.09.2014 E 14761644 (5)**

(97) Fecha y número de publicación de la concesión europea: **19.08.2020 EP 3047660**

(54) Título: **Método de comunicación entre un servidor y un elemento seguro**

(30) Prioridad:

**17.09.2013 EP 13306272**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**08.06.2021**

(73) Titular/es:

**THALES DIS FRANCE SA (100.0%)**
**6, rue de la Verrerie**
**92190 Meudon, FR**

(72) Inventor/es:

**EL-MAROUANI, ABDELLAH;**
**SINTZOFF, ANDRÉ;**
**GLOUSIEAU, JULIEN;**
**LANDIKOV, ILYAS;**
**RONFARD-HARET, CHRISTOPHE y**
**BERARD, XAVIER**

(74) Agente/Representante:

**ELZABURU, S.L.P**

## DESCRIPCIÓN

Método de comunicación entre un servidor y un elemento seguro

### Campo de la invención

La presente invención se refiere a métodos de comunicación entre un servidor y un elemento seguro a través de una red. Se refiere, concretamente, a los métodos de comunicación entre dos entidades en modo de punto a punto.

### Antecedentes de la invención

Los elementos seguros son pequeños dispositivos que comprenden una memoria, un procesador y un sistema operativo para tratamientos informáticos. Dichos elementos seguros pueden comprender una pluralidad de memorias de diferentes tipos, tales como memoria no volátil y memoria volátil. Se les llama “seguros” porque son capaces de controlar el acceso a los datos que contienen y de autorizar o no la utilización de datos por parte de otras máquinas. Los elementos seguros también pueden proporcionar servicios informáticos basados en componentes criptográficos. En general, los elementos seguros tienen recursos informáticos y recursos de memoria limitados y están destinados a ser conectados a una máquina anfitriona que les proporcione energía eléctrica. Los elementos seguros pueden ser extraíbles o ser fijos en una máquina anfitriona. Por ejemplo, las tarjetas inteligentes son un tipo de elementos seguros.

Un elemento seguro también puede ser implementado como una entidad virtual incrustada en un dispositivo a prueba de manipulaciones. Dicha entidad virtual se implementa en software y se comporta como un elemento seguro de hardware.

Se puede acceder a los elementos seguros mediante un servidor remoto a través de un canal inalámbrico, una red cableada, tal como Internet, o mediante una combinación de redes. El servidor remoto se comunica con un elemento seguro a través de una sesión de comunicación establecida a través de un enlace de punto a punto.

Un enlace de punto a punto es una conexión de comunicación establecida entre dos entidades. Esto es diferente de la topología de comunicación punto a multipunto o de difusión en la que varios receptores reciben información transmitida por un transmisor. Estas dos arquitecturas de comunicación pertenecen a dominios técnicos distintos, que tienen sus propias soluciones técnicas.

Algunos elementos seguros previstos para ser utilizados en el dominio de las telecomunicaciones o en el dominio de máquina a máquina (M2M) pueden gestionar un canal OTA (Inalámbrico - Over-The-Air, en inglés). También se puede acceder a estos elementos seguros a través del protocolo de transferencia de hipertexto, normalmente llamado HTTP (Hypertext Transfer Protocol, en inglés), o HTTPS, para el modo seguro. Por tanto, un servidor distante puede gestionar de manera remota el contenido de un elemento seguro tal como una UICC (Tarjeta universal de circuitos integrados – Universal Integrated Circuit Card, en inglés) a través de una sesión de comunicación dedicada, utilizando un protocolo específico. El servidor puede utilizar, por ejemplo, el mecanismo de RAM (Gestión de aplicaciones a distancia - Remote Applet Management, en inglés) definido por el estándar GlobalPlatform ® v 2.2 - Enmienda B “RAM over HTTP” o el protocolo OMA-DM (Alianza móvil abierta – Gestión de dispositivos - Open Mobile Alliance - Device Management, en inglés) definido por el protocolo tal como se define mediante el estándar OMA-TS-DM V1.2.1.

Un servidor remoto puede estar a cargo de desplegar datos en un grupo de elementos seguros ya desplegados en el campo. Por ejemplo, los datos a desplegar pueden ser una secuencia de comandos, una nueva aplicación, una actualización de una aplicación o, incluso, una actualización del propio sistema operativo. Los datos que se implementarán también pueden ser datos aplicativos, tales como un ajuste de una nueva configuración o datos secretos.

Algunos datos son adecuados para una configuración de un elemento seguro e incompatibles con una configuración diferente de otro elemento seguro. La configuración de un dispositivo puede depender de los componentes de hardware y/o de los elementos de software incrustados. Por ejemplo, la configuración puede estar definida por la versión del sistema operativo, por un perfil o por un dato específico instalado en el elemento seguro. El servidor se debe ocupar de cualquier inconsistencia entre la configuración del elemento seguro y los datos a enviar. Además, el servidor se debe comunicar con una gran cantidad de elementos seguros.

La diversidad de las configuraciones de los elementos seguros desplegados está aumentando considerablemente. Esta tendencia aumenta la complejidad del procesamiento que el servidor necesita realizar para implementar correctamente los datos en el conjunto existente de elementos seguros.

Es necesario mejorar la forma de gestionar el envío de datos desde un servidor a un elemento seguro distante.

La literatura que no es de patentes “OTA and Secure SIM Lifecyle Management” da a conocer el aprovisionamiento seguro de tarjetas SIM.

### Compendio de la invención

Un objetivo de la invención es resolver el problema técnico mencionado anteriormente.

El objetivo de la presente invención es un método de comunicación entre un servidor y un elemento seguro distante a través de un enlace de punto a punto. El elemento seguro distante comprende un valor de referencia. El método comprende:

- una etapa de proporcionar al servidor un conjunto que comprende una pluralidad de datos y una pluralidad de identificadores, estando asociado cada uno de dichos datos de la pluralidad de datos con un identificador que pertenece a la pluralidad de identificadores. La pluralidad de datos comprende un primer dato que es compatible con el elemento seguro distante, y un segundo dato que es incompatible con el elemento seguro distante.

- una etapa de enviar todo el conjunto desde el servidor al elemento seguro distante a través del enlace de punto a punto,

- en el elemento seguro distante, una etapa de realizar una operación de control con respecto al valor de referencia para cada identificador de la pluralidad de identificadores, y de descartar los datos asociados con los identificadores para los que falló la operación de control.

Ventajosamente, el elemento de seguridad distante puede haber sido emitido por un fabricante y puede tener un dispositivo de liberación. El valor de referencia puede reflejar el fabricante o la versión del dispositivo.

Ventajosamente, el elemento seguro distante puede comprender un sistema operativo que tiene una versión de lanzamiento y el valor de referencia puede reflejar la versión de lanzamiento.

Ventajosamente, un dato de la pluralidad de datos puede ser un componente ejecutable que es instalado en el elemento seguro distante en caso de una operación de control con éxito del identificador asociado con el componente ejecutable y el componente ejecutable puede modificar el comportamiento del sistema operativo.

Ventajosamente, el componente ejecutable puede ser un componente nativo.

De manera ventajosa, el identificador asociado con el componente nativo puede ser calculado utilizando una comprobación aleatoria (hash, en inglés) criptográfica de la versión de lanzamiento.

De manera ventajosa, un dato de la pluralidad de datos puede ser un comando que es ejecutado en el elemento seguro distante en caso de una operación de control con éxito del identificador asociado con el comando.

Ventajosamente, el elemento seguro distante puede generar una lista de todos los datos asociados con un identificador para los que falló la operación de control, y el elemento seguro distante puede enviar la lista al servidor.

Otro objeto de la invención es un servidor configurado para distribuir datos a un elemento seguro distante. El servidor incluye un conjunto que comprende una pluralidad de datos y una pluralidad de identificadores. Cada uno de dichos datos de la pluralidad de datos está asociado con un identificador que pertenece a la pluralidad de identificadores. La pluralidad de datos comprende tanto un primer dato compatible con el elemento seguro distante como un segundo dato incompatible con el elemento seguro distante. El servidor está configurado para enviar todo el conjunto al elemento seguro distante a través del enlace de punto a punto.

De manera ventajosa, un sistema puede comprender tanto el servidor de la invención como un conjunto de elementos seguros configurados para comunicarse de manera remota con el servidor. Cada uno de los elementos seguros puede comprender su propio valor de referencia y puede estar configurado para recibir el conjunto completo desde el servidor en modo de punto a punto. Cada elemento seguro del conjunto puede estar configurado para realizar una operación de control con respecto a su propio valor de referencia para cada identificador comprendido en el conjunto, y descartar los datos asociados con los identificadores para los que falló la operación de control.

**Breve descripción de los dibujos**

Otras características y ventajas de la presente invención surgirán más claramente de la lectura de la siguiente descripción de una serie de realizaciones preferentes de la invención, haciendo referencia a los dibujos adjuntos correspondientes, en los que:

- la figura 1 es un ejemplo de un servidor, según la invención;

- la figura 2 es un ejemplo de un elemento de seguridad, según la invención;

- la figura 3 representa un ejemplo de un sistema que comprende un servidor y un conjunto de elementos de seguridad, según la invención;

- la figura 4 muestra un ejemplo de un conjunto de datos enviados por el servidor, según la invención; y

- la figura 5 muestra otro ejemplo de un conjunto de datos enviados por el servidor, según la invención.

**Descripción detallada de las realizaciones preferentes**

La invención puede ser aplicada a cualquier tipo de servidor previsto para comunicarse con muchos elementos seguros que tengan diferentes configuraciones.

La invención puede ser aplicada a cualquier tipo de datos destinados a ser cargados en un elemento seguro. Por ejemplo, los datos cargados pueden ser archivos, páginas HTML, secuencias de comandos, aplicaciones, actualizaciones de aplicaciones, firmware, actualizaciones del sistema operativo, datos aplicativos o datos secretos.

La figura 1 muestra un ejemplo de un servidor SV, según la invención.

En este ejemplo, el servidor SV es una máquina informática que comprende una interfaz de comunicación IN2 capaz de comunicarse con cualquier elemento seguro perteneciente a un conjunto, FL (FLeet, en inglés), a través de un enlace de punto a punto. Por ejemplo, el servidor puede establecer un canal de comunicación a través de un OTA con un elemento seguro, tal como un UICC. En este caso, el servidor accede al elemento seguro a través de una máquina anfitriona, tal como un teléfono móvil. El servidor SV comprende un conjunto, ST (SeT, en inglés), que comprende datos D1 y D2 previstos para ser enviados a una pluralidad de elementos seguros. El dato D1 es compatible con un elemento seguro, mientras que el segundo dato D2 es incompatible con este elemento seguro. El segundo dato D2 es adecuado para otro elemento seguro de la flota FL.

El servidor SV comprende un elemento emisor M1 que está configurado para enviar todo el conjunto ST a cualquier elemento seguro SE1 conectado a través del enlace de punto a punto y perteneciente a la flota FL.

Por ejemplo, el conjunto ST puede ser una secuencia de comandos, y los datos D1 y D2 son comandos previstos para ser ejecutados en elementos seguros de la flota FL.

En otro ejemplo, los datos D1 y D2 pueden formar parte del código del sistema operativo o de una aplicación prevista para ser cargada mediante un comando de carga genérico.

El conjunto ST comprende los identificadores ID1 e ID2 que están asociados, respectivamente, con los datos D1 y D2.

El valor de cada uno de estos identificadores permite que un elemento seguro determine si los datos asociados son compatibles con su propia configuración. El identificador (también llamado etiqueta, indicador o marcador) puede ser codificado en uno o dos bytes, por ejemplo.

La figura 2 muestra un ejemplo de un elemento de seguridad SE1, según la invención.

El elemento seguro puede ser un dispositivo autónomo o un token electrónico conectado a una máquina anfitriona que proporciona acceso al servidor remoto SV. El elemento seguro también puede ser un elemento seguro virtual incrustado en un dispositivo a prueba de manipulaciones.

En concreto, el elemento seguro puede contener un procesador, una memoria no volátil, una memoria de trabajo y un sistema operativo. El S sistema operativo, OS (Operating System, en inglés), puede comprender una máquina virtual, en concreto una máquina virtual JavaCard®, una máquina virtual Java® o una máquina virtual .Net®. El procesador colabora con la memoria de trabajo y está diseñado para ejecutar el sistema operativo.

En el ejemplo de la figura 2, el elemento seguro SE1 es un dispositivo que comprende una interfaz de comunicación IN1, capaz de comunicarse a través de un enlace de punto a punto con el servidor SV de la figura 1. Esta interfaz de comunicación puede ser una interfaz sin contacto o de contacto. El elemento seguro SE1 pertenece al conjunto FL gestionado por el servidor distante.

El elemento seguro SE1 comprende un valor de referencia RV1 y un analizador M2, configurado para realizar una operación de control con respecto a su propio valor de referencia RV1 para cada identificador comprendido en el conjunto recibido del servidor SV. El analizador M2 está configurado para descartar los datos asociados con los identificadores para los que falló la operación de control. En otras palabras, el analizador M2 garantiza que los datos que no son compatibles con el elemento seguro SE1 no son ejecutados ni almacenados de manera permanente en el elemento seguro SE1.

Haciendo referencia al ejemplo del conjunto ST de la figura 1, el analizador M2 utiliza el valor de referencia RV1 para determinar qué comando es adecuado para el elemento seguro SE1. En una realización preferente, el analizador M2 simplemente compara el valor de cada identificador con el valor de referencia RV1 para tomar una decisión.

En un ejemplo, el valor de referencia RV1 puede reflejar la versión de lanzamiento del sistema operativo del elemento seguro SE1.

En otro ejemplo, el valor de referencia RV1 puede reflejar la versión del dispositivo del elemento seguro SE1. La versión del dispositivo corresponde a la combinación de características de hardware y/o software del elemento seguro. La versión del dispositivo puede estar definida por el conjunto de capacidades del elemento seguro.

Por ejemplo, la versión del dispositivo puede corresponder al número de generación del elemento seguro (es decir, un número que identifica el rango al que pertenece el elemento seguro) o un número calculado específico asociado con el elemento seguro. La versión del dispositivo también puede variar según la presencia de un componente que proporcione una característica específica, tal como NFC o funciones criptográficas. La versión del dispositivo también puede corresponder a una versión de estándar implementada en el elemento seguro.

En otro ejemplo, el valor de referencia RV1 puede reflejar el fabricante que suministra el elemento seguro.

En otro ejemplo, el valor de referencia RV1 puede reflejar cualquier combinación de los criterios mencionados anteriormente.

En otras palabras, el valor de referencia permite identificar la configuración del elemento seguro.

El elemento seguro SE1 puede comprender un medio de notificación M3, configurado para generar un informe que refleje el resultado de todas las operaciones de control realizadas por el analizador M2. Por ejemplo, el medio de notificación M3 puede construir una lista que comprenda una referencia a los datos del conjunto recibido para el cual la operación de control se realizó correctamente. Alternativamente, la lista puede corresponder a los datos del conjunto recibido para el que falló la operación de control.

Ventajosamente, el analizador M2 puede realizar la operación de control ejecutando una función que es más compleja que una simple operación de comparación. Por ejemplo, el analizador M2 puede aplicar el identificador a una función criptográfica, para obtener un resultado que, a continuación, es comparado con el valor de referencia.

Ventajosamente, el analizador M2 puede ser configurado para borrar inmediatamente los datos asociados con un identificador cuya operación de control falló.

El sistema operativo del elemento seguro puede depender de componentes nativos. Un componente nativo es un componente de software desarrollado en un lenguaje específico del microprocesador integrado. Esta redacción específica significa que un componente nativo no se desarrolla en un lenguaje asociado con una máquina virtual, tal como el lenguaje Java ©. Por ejemplo, un componente nativo puede ser desarrollado en lenguaje de ensamblador o en lenguaje C. Por tanto, un componente nativo no es un componente genérico y no es compatible con una gran cantidad de plataformas de hardware.

En otro ejemplo, el conjunto ST comprende una colección de componentes nativos correspondientes a diferentes objetivos de hardware. Cada identificador puede ser el resultado de la función de comprobación aleatoria criptográfica de una parte (o de la totalidad) del sistema operativo objetivo. Por tanto, el analizador M2 puede realizar la operación de control calculando la comprobación aleatoria del sistema operativo almacenado en el elemento seguro y comparando la comprobación aleatoria calculada con cada identificador recibido.

Ventajosamente, el identificador puede ser calculado utilizando una función específica, teniendo en cuenta una comprobación aleatoria del sistema operativo objetivo como parámetro de entrada. Por ejemplo, la función específica puede ser la concatenación de la comprobación aleatoria y de una referencia de la versión del dispositivo, tal como se detalló anteriormente.

En otro ejemplo, el identificador puede estar basado en la versión de construcción que produjo el sistema operativo activo en el elemento seguro.

En otro ejemplo, el conjunto ST comprende una colección de componentes desarrollados en un lenguaje de alto nivel, tal como JavaCard ©, y correspondientes a diferentes versiones de máquinas virtuales. El conjunto ST también puede comprender una colección que mezcla componentes nativos y componentes desarrollados en un lenguaje de alto nivel.

La invención permite proteger los elementos seguros desplegados, evitando modificaciones no deseadas de su comportamiento, ya que ahora cada elemento seguro puede recuperar los datos correctos entre todo el conjunto recibido del servidor.

La figura 3 muestra un ejemplo de un sistema SY que comprende un servidor SV y un conjunto FL de elementos seguros, según la invención.

En este ejemplo, el servidor SV es similar al servidor descrito en la figura 1. El servidor SV comprende un conjunto ST de datos destinados a ser distribuidos a cada elemento seguro del conjunto FL.

En este ejemplo, el conjunto FL comprende cuatro elementos seguros SE1, SE2, SE3 y SE4. Cada uno de estos elementos seguros tiene una arquitectura similar a la descrita en la figura 2. Cada uno de estos elementos seguros comprende su propio valor de referencia. Por ejemplo, los elementos seguros SE1 y SE2 pueden tener el mismo valor de referencia correspondiente a la versión 1.2 del sistema operativo, mientras que el elemento seguro SE3 tiene un valor de referencia correspondiente a la versión 1.3, y el elemento seguro SE4 tiene un valor de referencia correspondiente a la versión 1.5.

Ventajosamente, el servidor SV se puede comunicar con múltiples conjuntos de elementos seguros y gestionar tantos conjuntos de datos diferentes para distribuir.

La figura 4 muestra un ejemplo de un conjunto ST2 de datos enviados por el servidor SV a los elementos seguros del conjunto FL.

En este ejemplo, el conjunto ST2 es una secuencia de comandos ordenados. La secuencia de comandos comprende dos comandos D3 y D4 que están asociados con el identificador ID3, un comando D5 asociado con el identificador ID4 y tres comandos D6, D7 y D8 que están asociados con el identificador ID5. El identificador ID3 tiene un valor correspondiente a la versión 1.2 del sistema operativo, mientras que el identificador ID4 tiene un valor correspondiente a la versión 1.3, y el identificador ID5 tiene un valor correspondiente a la versión 1.5.

Haciendo referencia al ejemplo de la flota FL de la figura 3, los elementos seguros SE1 y SE2 recibirán el conjunto completo ST2 y ejecutarán los comandos D3 y D4 que están asociados con el identificador ID3. Descartarán los comandos D5 a D8. De la misma forma, el elemento seguro SE3 ejecutará el comando D5 y descartará los demás comandos de la secuencia. Los elementos seguros SE4 recibirán el conjunto completo ST2 y ejecutarán los comandos D6, D7 y D8 y descartarán los comandos D3 a D5.

La figura 5 muestra un ejemplo de un conjunto ST3 de datos enviados por el servidor SV a los elementos seguros del conjunto FL.

En este ejemplo, el conjunto ST3 es una secuencia de comandos ordenados. La secuencia comprende un comando D9 que está asociado con los identificadores IDA e IDB, un comando D10 asociado con el identificador IDB y un comando D11 asociado con los identificadores IDA, IDB e IDC.

El identificador IDA tiene un valor correspondiente a la versión 1.5 del sistema operativo, mientras que el identificador IDB tiene un valor correspondiente a la versión 1.3, y el identificador IDC tiene un valor correspondiente a la versión 1.1.

Haciendo referencia al ejemplo del conjunto FL de la figura 3, los elementos seguros SE1 y SE2 recibirán el conjunto ST3 completo y descartarán todos los comandos de la secuencia sin ejecutar ningún comando. Esto se debe al hecho de que ningún comando está asociado con un identificador que tenga un valor correspondiente al valor de referencia de estos elementos seguros. El elemento seguro SE3 ejecutará los comandos D9, D10 y D11. El elemento seguro SE4 ejecutará los comandos D9 y D11, únicamente.

Ventajosamente, el conjunto enviado por el servidor puede comprender un identificador comodín que indica que los datos adjuntos al mismo están previstos para todos los destinatarios.

En el caso de un elemento seguro del tipo UICC, el identificador puede ser implementado utilizando el formato de datos de Aplicación Remota Expandida que se define en el estándar TS 102.226 Versión 9 o superior. Los TLV de comando (Valor de la longitud de la etiqueta - Tag-Length-Value, en inglés) que están en el encadenamiento de comandos pueden ser utilizados para transmitir el identificador. Estos TLV de comando se describen en la versión estándar 9 o superior de TS 102.223. En concreto, el mecanismo de Comprensión-TLV (C-TLV) se puede ampliar para gestionar el identificador.

Gracias a la invención, el servidor puede gestionar una única versión del conjunto de datos a enviar independientemente de la diversidad de los elementos seguros objetivo. No hay riesgo de que un elemento seguro intente ejecutar un comando no soportado enviado por el servidor, sabiendo que dicho intento de ejecución puede conducir a un bloqueo definitivo del elemento seguro. De este modo, la invención evita que una descarga incorrecta pueda dañar definitivamente un elemento seguro que no puede ser reemplazado, por ejemplo, si el elemento seguro está soldado en un dispositivo anfitrión.

Gracias a la invención, ya no es necesario que el servidor gestione contenido específicamente diseñado para cada envío de datos a un elemento seguro.

La invención permite una autoprotección de un elemento seguro evitando actualizaciones erróneas y peligrosas de su propia configuración.

**REIVINDICACIONES**

1. Un método de comunicación entre un servidor (SV) y un elemento seguro (SE1) distante a través de un enlace de punto a punto, comprendiendo dicho elemento seguro (SE1) distante un valor de referencia (RV1), comprendiendo dicho método las siguientes etapas:

- proporcionar al servidor (SV) un conjunto (ST) que comprende una pluralidad de datos (D1, D2) y una pluralidad de identificadores (ID1, ID2), estando asociado cada uno de dichos datos de la pluralidad de datos (D1, D2) con un identificador perteneciente a la pluralidad de identificadores (ID1, ID2),
- enviar todo el conjunto (ST) desde el servidor (SV) al elemento seguro (SE1) distante a través del enlace de punto a punto,
- en el elemento seguro distante (SE1), realizar una operación de control con respecto al valor de referencia (RV1) para cada identificador de la pluralidad de identificadores (ID1, ID2), y descartar los datos asociados con los identificadores para los que falló la operación de control,

y caracterizado por que dicha pluralidad de datos (D1, D2) comprende un primer dato (D1) compatible con el elemento seguro (SE1) distante y un segundo dato (D2) incompatible con el elemento seguro (SE1) distante.

2. Un método, según la reivindicación 1, en el que la operación de control se realiza comprobando que cada uno de dichos identificadores está vinculado individualmente al valor de referencia mediante una función criptográfica predefinida que es ejecutada por el elemento seguro distante.

3. Un método, según la reivindicación 1, en el que el elemento de seguridad (SE1) distante ha sido suministrado por un fabricante y tiene una versión de dispositivo, y en el que dicho valor de referencia (RV1) refleja el fabricante o la versión del dispositivo.

4. Un método, según la reivindicación 1, en el que el elemento de seguridad (SE1) distante comprende un sistema operativo que tiene una versión de lanzamiento, y en el que dicho valor de referencia (RV1) refleja la versión de lanzamiento.

5. Un método, según la reivindicación 4, en el que un dato de la pluralidad de datos (D1, D2) es un componente ejecutable que es instalado en el elemento seguro (SE1) distante en caso de operación de control con éxito del identificador asociado con el componente ejecutable, y en el que el componente ejecutable modifica el comportamiento de dicho sistema operativo.

6. Un método, según la reivindicación 5, en el que el componente ejecutable es un componente nativo.

7. Un método, según la reivindicación 6, en el que el identificador asociado con el componente nativo se calcula utilizando una comprobación aleatoria criptográfica de la versión de lanzamiento.

8. Un método, según la reivindicación 1, en el que un dato de la pluralidad de datos (D1, D2) es un comando que se ejecuta en el elemento seguro (SE1) distante en caso de operación de control con éxito del identificador asociado con el comando.

9. Un método, según la reivindicación 1, en el que el elemento seguro (SE1) distante genera una lista de todos los datos asociados con un identificador para el que falló la operación de control, y en el que el elemento seguro (SE1) distante envía la lista al servidor (SV).

10. Un servidor (SV), configurado para distribuir datos a un elemento seguro (SE1) distante, comprendiendo el servidor un conjunto (ST) que comprende una pluralidad de datos (D1, D2) y una pluralidad de identificadores (ID1, ID2), estando asociados cada uno de dichos datos de la pluralidad de datos (D1, D2) con un identificador perteneciente a la pluralidad de identificadores (ID1, ID2), en el que el servidor (SV) está configurado para enviar el conjunto completo (ST) al elemento seguro (SE1) distante a través del enlace de punto a punto,

y caracterizado por que dicha pluralidad de datos (D1, D2) comprende un primer dato (D1) compatible con el elemento seguro (SE1) distante y un segundo dato (D2) incompatible con el elemento seguro (SE1) distante.

11. Un sistema (SY), que comprende el servidor (SV) de la reivindicación 10 y un conjunto (FL) de elementos seguros configurados para comunicarse de manera remota con el servidor (SV), donde cada uno de dichos elementos seguros comprende su propio valor de referencia y está configurado para recibir todo el conjunto (ST) desde el servidor (SV) en modo de punto a punto, y en el que cada elemento seguro de dicho conjunto (FL) está configurado para realizar una operación de control con respecto a su propio valor de referencia para cada identificador comprendido en el conjunto (ST) y descartar los datos asociados con los identificadores para los que falló la operación de control.

12. Un sistema, según la reivindicación 11, en el que cada elemento seguro de dicho conjunto está configurado para realizar la operación de control, comprobando que cada uno de dichos identificadores está vinculado individualmente al propio valor de referencia mediante una función criptográfica predefinida.

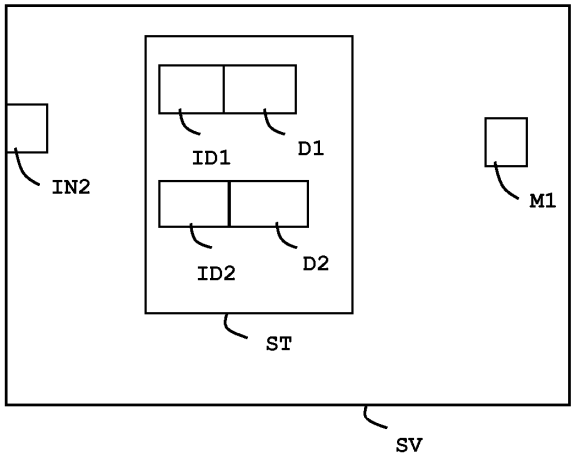


FIG. 1

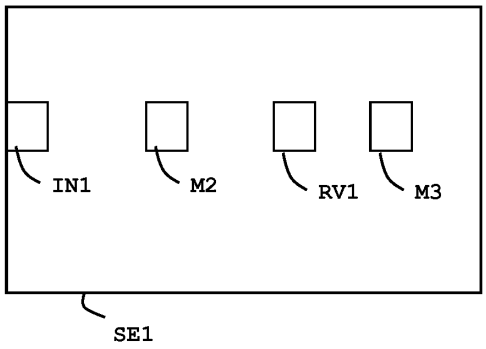


FIG. 2

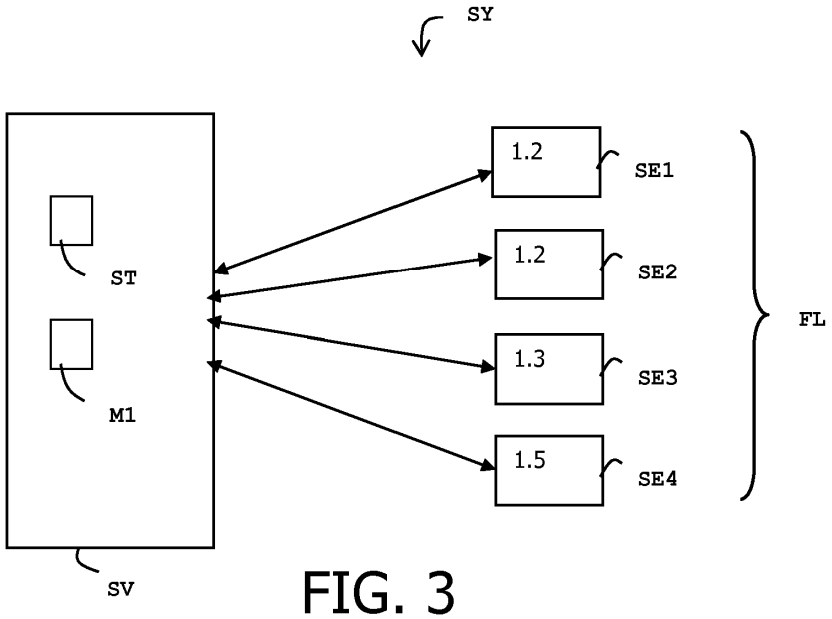


FIG. 3

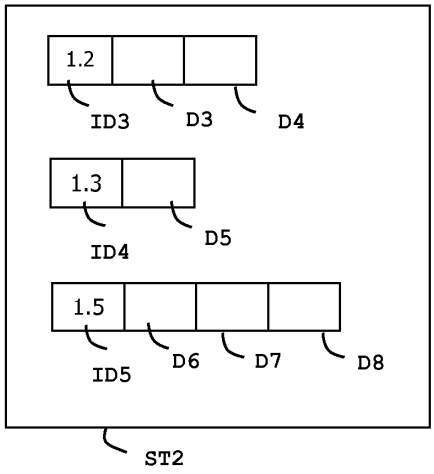


FIG. 4

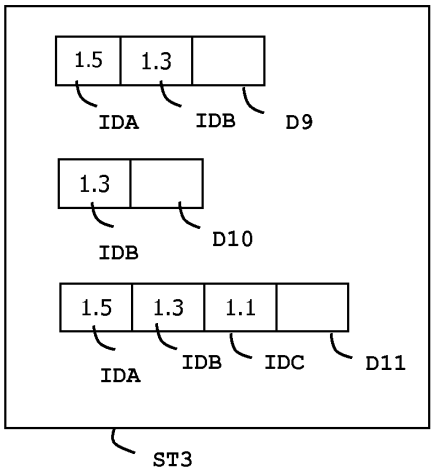


FIG. 5