(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 857 674**

(51) Int. CI.:

H04W 12/04 (2011.01)
H04W 12/00 (2011.01)
G06F 16/16 (2009.01)
G06F 21/72 (2013.01)
G06Q 20/34 (2012.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.11.2014 E 14306865 (8)**

(97) Fecha y número de publicación de la concesión europea: **27.01.2021 EP 3023904**

(54) Título: **Creación de archivos implícita en secuencias de comandos APDU**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.09.2021

(73) Titular/es:

IDEMIA FRANCE (100.0%)
2 Place Samuel de Champlain
92400 Courbevoie, FR

(72) Inventor/es:

DUMOULIN, JÉRÔME y
WOZNIAK, TOMASZ

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

ES 2 857 674 T3

DESCRIPCIÓN

Creación de archivos implícita en secuencias de comandos APDU

ANTECEDENTES

Existe un creciente interés en las comunicaciones de máquina a máquina (M2M) en las que una máquina se comunica con otra máquina a través de una red de comunicaciones. Los dispositivos M2M se pueden proporcionar con una tarjeta de circuito integrado universal incrustada (eUICC). La eUICC realiza funciones similares a las realizadas por una tarjeta de un módulo de identidad de abonado (SIM) en un dispositivo inalámbrico personal. Sin embargo, la eUICC no es tan fácil de quitar ya que está incrustada en el dispositivo, soldándose, por ejemplo, en una placa de circuito del dispositivo.

Se está desarrollando una arquitectura para el aprovisionamiento y la gestión remotos de dispositivos con una UICC incrustada. Un organismo de normalización activo en esta área es la Asociación GSM (GSMA), que desarrolló la especificación "Remote Provisioning Architecture for Embedded UICC, Technical Specification". Una versión temprana de esta especificación es la versión 2.0, con fecha 13 de octubre de 2014.

Parte del proceso para proveer un dispositivo eUICC es instalar un perfil en el dispositivo. El perfil proporciona al dispositivo la funcionalidad para acceder a una infraestructura de red móvil específica. El perfil puede comprender una estructura de archivos, datos y aplicaciones. El perfil se puede proveer de forma remota en la eUICC.

Una vez que una eUICC está en su "fase de uso", toda la comunicación entre la eUICC y el mundo exterior se lleva a cabo a través de comandos APDU ISO 7816. La eUICC recibe un APDU y devuelve una respuesta. La especificación técnica TS 102 226 del Instituto Europeo de Normas de Telecomunicación (ETSI), "Remote APDU structure for UICC based applications", define protocolos que permiten a entidades remotas enviar una secuencia de comandos a una UICC. La secuencia de comandos contiene una serie de comandos APDU y la secuencia de comandos está dirigida a una aplicación en la tarjeta, denominada en la especificación ETSI "aplicación de gestión remota".

En el contexto del aprovisionamiento remoto, se crea un perfil cuando una aplicación de gestión remota en la tarjeta ejecuta los comandos en una "secuencia de comandos de aprovisionamiento". Una eUICC puede almacenar múltiples perfiles, tal como un perfil por tipo de red de acceso (GSM, CDMA). Además, se puede actualizar un perfil o descargar un nuevo perfil cuando el propietario de un dispositivo inalámbrico desea usar un operador de red de acceso diferente para proporcionar la red de acceso a ese dispositivo inalámbrico.

A medida que aumenta el número de perfiles y su complejidad, las secuencias de comandos para crearlos se vuelven progresivamente más grandes. El documento EP 1 605 415 A1 (AXALTO SA [FR]) 14 de diciembre de 2005 (14/12/2005) desvela operaciones de gestión de archivos en una tarjeta inteligente. En la inicialización del subprograma (*applet*) (primera invocación), el código trata de seleccionar sucesivamente los archivos necesarios. Si el archivo no está allí, se crea y se rellena con los datos de personalización solicitados. Por lo tanto, no es necesario crear los archivos durante la personalización. Los parámetros de archivos necesarios están integrados en el código. El documento EP 2 447 835 A1 (OBERTHUR TECHNOLOGIES [FR]) 2 de mayo de 2012 (02/05/2012) desvela un procedimiento para la personalización rápida (previa) de tarjetas SIM. Los comandos propietarios o reutilizados en una secuencia de comandos incluyen un identificador (puntero a una dirección en E2PROM) para una ubicación en ROM. La ubicación en ROM contiene una librería de secuencias de comandos o parámetros específicos de archivo que pueden almacenarse cifrados. Por lo tanto se reduce el número de comandos enviados a la tarjeta. Se utiliza para la personalización previa (protocolos de configuración, tamaño de E2PROM o velocidad de UC) o la personalización (mismos datos que en los comandos CREATE FILE (creación de archivo) o UPDATE BINARY (actualización binaria)).

RESUMEN

La invención se define mediante las reivindicaciones independientes adjuntas. Las reivindicaciones dependientes describen diferentes formas de realización.

Un aspecto de la invención proporciona un procedimiento para preparar una secuencia de comandos que enviar a un elemento de seguridad para proveer de forma remota un perfil en un elemento de seguridad, donde el elemento de seguridad tiene un almacenamiento local de datos de propiedad de archivo, comprendiendo el procedimiento preparar la secuencia de comandos de modo que la secuencia de comandos carezca de un comando para crear un archivo si el almacenamiento local de datos de propiedad de archivo en el elemento de seguridad incluye datos de propiedad de archivo que se pueden usar para crear localmente ese archivo.

El procedimiento se puede realizar para crear o generar una secuencia de comandos que enviar a un elemento de seguridad, tal como crear una secuencia de comandos a partir de un archivo de especificación. De manera alternativa, el procedimiento se puede realizar para procesar o "filtrar" una secuencia de comandos existente. Al procesar la secuencia de comandos existente, el procedimiento puede reducir la longitud de la secuencia de comandos.

La secuencia de comandos puede comprender una entrada que identifica el archivo que se creará localmente en el elemento de seguridad. La entrada puede tener una longitud más corta que una entrada que incluye un comando de creación de archivo. Por ejemplo, una entrada con un comando de creación de archivo también necesita especificar varios parámetros para crear el archivo.

El procedimiento puede comprender: recibir una primera secuencia de comandos que comprende una primera entrada que comprende un comando para crear un archivo; determinar si la primera entrada en la secuencia de comandos corresponde a un archivo cuyas propiedades de archivo están almacenadas en el almacenamiento local de datos de propiedad de archivo en el elemento de seguridad; si la primera entrada corresponde al archivo cuyas propiedades de archivo están almacenadas, reemplazar la primera entrada en la secuencia de comandos por una segunda entrada en la secuencia de comandos, donde la segunda entrada es más corta que la primera entrada y carece del comando para crear el archivo; y proporcionar una secuencia de comandos modificada de menor longitud que la primera secuencia de comandos.

La primera entrada puede comprender un comando de creación de archivo, un identificador de archivo y propiedades de archivo, y la segunda entrada puede comprender el identificador de archivo. La segunda entrada no necesita especificar todas, o ninguna, de las propiedades de archivo.

La segunda entrada puede comprender un comando de selección de archivo.

Otro aspecto de la invención proporciona un procedimiento para proveer un perfil en un elemento de seguridad, que comprende:

recibir una secuencia de comandos para proveer el perfil;
ejecutar la secuencia de comandos para proveer el perfil, donde la ejecución comprende:
leer una entrada en la secuencia de comandos que se refiere a un archivo;
determinar si el archivo existe; y, si el archivo no existe, crear el archivo usando un almacenamiento local de datos de propiedad de archivo en el elemento de seguridad.

La entrada en la secuencia de comandos puede comprender un identificador de archivo y el procedimiento comprende: usar el identificador de archivo para localizar datos de propiedad de archivo en el almacenamiento local; y crear el archivo con el identificador y los datos de propiedad de archivo.

La entrada en la secuencia de comandos puede comprender un comando de selección de archivo.

Otro aspecto de la invención proporciona un procedimiento para proveer un perfil en un elemento de seguridad, que comprende:

recibir una secuencia de comandos para proveer el perfil y
ejecutar la secuencia de comandos para proveer el perfil;

el procedimiento comprende además, antes de ejecutar la secuencia de comandos, crear al menos un archivo requerido por el perfil usando un almacenamiento local de datos de propiedad de archivo en el elemento de seguridad, y donde la secuencia de comandos recibida carece de un comando para crear el al menos un archivo.

La entrada en la secuencia de comandos puede comprender un comando de selección de archivo y un identificador de archivo, y el archivo creado antes de la ejecución de la secuencia de comandos puede comprender el mismo identificador de archivo.

Crear al menos un archivo requerido por el perfil puede comprender crear al menos un archivo obligatorio.

El procedimiento puede comprender además recibir una tabla de servicio que indica al menos un servicio requerido por el perfil, y donde el almacenamiento local de datos de propiedad de archivo incluye una indicación de un servicio al que están asociados los datos de propiedad de archivo, y el procedimiento comprende:

utilizar la tabla de servicios para identificar un servicio requerido para el perfil;
recuperar datos de propiedad de archivo del almacenamiento local de datos de propiedad de archivo para cada servicio requerido; y
crear al menos un archivo para el servicio requerido usando los datos de propiedad de archivo recuperados.

Los datos de propiedad de archivo pueden comprender al menos uno de: un identificador de archivo, un tamaño de archivo y derechos de acceso a archivo.

Los datos de propiedad de archivo se pueden almacenar en una única estructura de datos que almacena datos de propiedad de archivo para archivos obligatorios y archivos opcionales. La estructura de datos puede indexarse de acuerdo con el número de servicio. Por ejemplo, los archivos obligatorios pueden identificarse mediante un número de servicio = 0 o un número negativo, y los archivos opcionales mediante un número de servicio ≥1.

El elemento de seguridad puede ser una tarjeta de circuito integrado universal incrustada.

Los comandos en la secuencia de comandos pueden cumplir la norma ISO 7816.

Los procedimientos realizados en el elemento de seguridad se consideran soluciones alternativas a un problema técnico particular.

Una ventaja de al menos una forma de realización es que el tamaño de la secuencia de comandos puede reducirse. Una ventaja de al menos una forma de realización es que el tamaño de la secuencia de comandos se puede reducir al tiempo que se mantiene la conformidad con los comandos existentes utilizados a través de una interfaz con el dispositivo. Por ejemplo, la secuencia de comandos puede seguir cumpliendo la norma ISO 7816 porque sigue utilizando comandos APDU ISO 7816.

La funcionalidad descrita aquí puede implementarse en hardware, software ejecutado por un aparato de procesamiento o por una combinación de hardware y software. El aparato de procesamiento puede comprender un ordenador, un procesador, una máquina de estados, una matriz lógica o cualquier otro aparato de procesamiento adecuado. El aparato de procesamiento puede ser un procesador de propósito general que ejecuta software para hacer que el procesador de propósito general realice las tareas requeridas, o el aparato de procesamiento puede estar dedicado a realizar las funciones requeridas. Otro aspecto de la invención proporciona instrucciones legibles por máquina (software) que, cuando son ejecutadas por un procesador, realizan cualquiera de los procedimiento descritos o reivindicados. Las instrucciones legibles por máquina pueden almacenarse en un dispositivo de memoria electrónica, disco duro, disco óptico u otro medio de almacenamiento legible por máquina. El medio legible por máquina puede ser un medio legible por máquina no transitorio. El término "medio legible por máquina no transitorio" comprende todos los medios legibles por máquina excepto una señal de propagación transitoria. Las instrucciones legibles por máquina se pueden descargar al medio de almacenamiento a través de una conexión de red.

Otro aspecto de la invención proporciona un elemento de seguridad que comprende un procesador y una memoria, donde la memoria contiene instrucciones ejecutables por el procesador, mediante las cuales el procesador está configurado para realizar la funcionalidad descrita o reivindicada con respecto al elemento de seguridad.

Otro aspecto de la invención proporciona un aparato para su uso en la preparación de una secuencia de comandos, donde el aparato comprende un procesador y una memoria, donde la memoria contiene instrucciones ejecutables por el procesador, mediante las cuales el procesador está configurado para realizar la funcionalidad en el lado servidor descrita o reivindicada.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Se describirán formas de realización de la invención, solo a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

La Figura 1 muestra una arquitectura para el aprovisionamiento y gestión de una tarjeta de circuito integrado universal incrustada (eUICC);
la Figura 2 muestra un ejemplo de aprovisionamiento remoto de un perfil en una eUICC;
la Figura 3 muestra un extracto de un ejemplo de una secuencia de comandos convencional para proveer un perfil en una eUICC;
la Figura 4 muestra un extracto de un ejemplo de una secuencia de comandos modificada para proveer un perfil en una eUICC;
la Figura 5 muestra un ejemplo de un procedimiento realizado por una aplicación de gestión en una eUICC;
la Figura 6 muestra un ejemplo de una tabla de propiedades de archivo utilizada por la aplicación de gestión;
la Figura 7 muestra otro ejemplo de un procedimiento realizado por una aplicación de gestión en una eUICC;
la Figura 8 muestra otro ejemplo de una tabla de propiedades de archivo utilizada por la aplicación de gestión;
la Figura 9 muestra un procedimiento para preparar una secuencia de comandos para proveer un perfil;
la Figura 10 muestra un ejemplo de aparato en una eUICC.

DESCRIPCIÓN DETALLADA

La Figura 1 muestra una arquitectura para el aprovisionamiento y gestión de una tarjeta de circuito integrado universal incrustada (eUICC) 30 alojada en un dispositivo inalámbrico 20. Ejemplos del dispositivo inalámbrico 20 son un dispositivo de máquina a máquina (M2M) y un dispositivo móvil, tal como un teléfono inteligente, un teléfono móvil, una llave USB (*dongle*) u otro dispositivo inalámbrico que puede comunicarse a través de una red inalámbrica. El dispositivo 20 utiliza al menos una red de acceso inalámbrico, tal como una red 2G, 3G o 4G. La eUICC 30 es un ordenador autónomo en un chip con un procesador y almacenamiento. La eUICC 30 proporciona un entorno seguro en el que realizar determinadas tareas, tal como establecer una comunicación segura con la red de acceso.

Un perfil se puede proveer de forma remota a la eUICC 30. El perfil proporciona al dispositivo la funcionalidad para acceder a una infraestructura de red móvil específica. El perfil puede comprender una estructura de archivos, datos y aplicaciones. Las entidades de red que participan en el proceso de aprovisionamiento incluyen una entidad de preparación de datos de gestor de suscripciones (SM-DP) 10 y una entidad de encaminamiento seguro de gestor de suscripciones (SM-SR) 12. La SM-DP 10 prepara los perfiles y gestiona la descarga e instalación seguras de los perfiles en la eUICC 30. La SM-SR 12 realiza de forma segura funciones de comandos de gestión de plataforma y el transporte de comandos de gestión de perfiles. Se utiliza una red de comunicación 15 para acceder al dispositivo 30 con fines de aprovisionamiento. Una eUICC puede almacenar múltiples perfiles 31. La eUICC 30 también puede almacenar una tabla de propiedades de archivo (FP) 50. Como se describe con más detalle más adelante, la tabla de propiedades de archivo 50 se utiliza al proveer un perfil. La tabla de propiedades de archivo 50 puede ser utilizada como recurso compartido por la eUICC al proveer uno o más perfiles 31.

El almacenamiento de datos de propiedad de archivo 50 se puede transferir al eUICC 30 durante la fabricación del eUICC, o durante la expedición previa de la eUICC o dispositivo anfitrión 20 en el que se incrusta la eUICC.

La Figura 2 muestra un ejemplo de aprovisionamiento remoto de un perfil en una eUICC 30. En el contexto del aprovisionamiento remoto, se crea un perfil cuando una aplicación de gestión remota en la tarjeta ejecuta los comandos en una secuencia de comandos de aprovisionamiento. La SM-DP 10 prepara una secuencia de comandos. La secuencia de comandos se cifra de acuerdo con un protocolo estándar, tal como SCP03, y se dirige a una aplicación de gestión remota, RM1, en la eUICC 30. La RM1 se ejecuta en un entorno seguro, perfil de dominio de seguridad de expedidor (ISD-P), que está controlado por la entidad que controla el perfil, que generalmente será un operador de red móvil. Hay una clave SCP03 compartida en la eUICC 30 y la SM-DP 10 que ya habrá sido implementada por el operador de red móvil antes de que se pueda dirigir cualquier secuencia de comandos a la RM1. Cuando la RM1 recibe una secuencia de comandos, la descifra y ejecuta los comandos contenidos en la secuencia de comandos, lo que crea un perfil.

La secuencia de comandos se encamina a través de la SM-SR 12. La SM-SR 12 recibe una secuencia de comandos cifrada desde la SM-DP 10, cifra la secuencia de comandos de acuerdo con un protocolo estándar, por ejemplo, SCP80 o SCP81, y la dirige a una RM2. La RM2 se ejecuta en un entorno seguro, raíz de dominio de seguridad de expedidor (ISD-R), que generalmente está controlado por el expedidor de la eUICC 30. Hay una clave SCP80/SCP81 compartida en la eUICC 30 y la SM-SR 12 que habrá sido implementada por el expedidor de tarjetas antes de que se pueda dirigir cualquier secuencia de comandos a la RM2. Cuando la RM2 recibe una secuencia de comandos, la descifra y la reenvía a la RM1.

La Figura 3 muestra un extracto corto de un ejemplo de una secuencia de comandos convencional 40. La secuencia de comandos convencional 40 incluye entradas 41, 42, 43 que indican a la eUICC que cree un archivo. Las entradas comprenden un comando "CREATE FILE" (crear archivo), un identificador del archivo que se creará y propiedades/parámetros para la creación de archivos.

La Figura 4 muestra un extracto corto de un ejemplo de una secuencia de comandos modificada 45. En la secuencia de comandos modificada 45, las entradas 41, 42, 43 se han reemplazado por entradas más cortas 46, 47, 48. Las entradas más cortas 46, 47, 48 indican a la eUICC que seleccione un archivo. Cada entrada 46, 47, 48 incluye un identificador del archivo que se seleccionará. Por ejemplo, la entrada 46 indica a la eUICC que seleccione un archivo con el identificador 2F06. Una forma ventajosa de las entradas más cortas 46, 47, 48 consiste en un comando SELECT FILE (seleccionar archivo) y un identificador del archivo, y no especifica ninguna propiedad de archivo. La secuencia de comandos modificada 45 es más corta que la secuencia de comandos convencional 40 porque las entradas 41, 42, 43 se han reemplazado por entradas más cortas 46, 47, 48. La reducción de tamaño se ha logrado de una manera que es compatible con una secuencia de comandos convencional. Por ejemplo, la secuencia de comandos modificada 45 utiliza comandos APDU convencionales (ISO 7816) en las ubicaciones donde se ha modificado. La reducción en tamaño es posible porque la eUICC tiene un almacenamiento local 50 de datos de propiedad de archivo que permite que la eUICC cree el archivo requerido. Otras entradas en la secuencia de comandos después de una entrada 46, 47, 48 pueden especificar datos para rellenar un archivo. Los datos pueden especificarse en una o más entradas "UPDATE RECORD" (actualizar registro) de la secuencia de comandos.

De manera ventajosa, la secuencia de comandos modificada incluye una cabecera que indica que la secuencia de comandos es una secuencia de comandos modificada. Esto permite que la eUICC 30 procese la secuencia de comandos de una manera adecuada.

La aplicación de gestión en la eUICC puede funcionar en una de varias maneras posibles de acuerdo con la secuencia de comandos modificada 45. A continuación se describirá un primer ejemplo de funcionamiento de la aplicación de gestión en la eUICC con referencia a la Figura 5. En el bloque 101 se recibe una secuencia de comandos en la eUICC 30. La secuencia de comandos puede ser de la forma de la secuencia de comandos 45 mostrada en la Figura 4. En el bloque 102, la secuencia de comandos se ejecuta línea por línea. En el bloque 103, la aplicación de gestión alcanza una entrada en la secuencia de comandos que incluye un comando SELECT FILE (seleccionar archivo) y una referencia a un archivo. Por ejemplo, el comando SELECT FILE puede identificar el archivo que se seleccionará, como en las entradas de ejemplo 46, 47, 48 de la Figura 4. El bloque 104 comprueba si el archivo especificado en el comando SELECT FILE existe. Si el archivo existe, el procedimiento puede proceder como de costumbre y la ejecución continúa. Si el archivo no existe, el procedimiento avanza hasta el bloque 105 y genera y ejecuta un comando CREATE FILE para crear el archivo requerido en el bloque 104. El bloque 105 utiliza la tabla de propiedades de archivo (FP) almacenada localmente (50, Fig. 1) que incluye parámetros que se utilizarán al crear los archivos. La tabla FP 50 puede incluir, por ejemplo, identidad de archivo, derechos de acceso y tamaño.

La Figura 6 muestra una tabla FP 50 de ejemplo para su uso con la secuencia de comandos modificada 45 de la Figura 4. Cada entrada 51, 52, 53 en la tabla 50 corresponde a un archivo que se creará. Haciendo de nuevo referencia a la secuencia de comandos de la Figura 4, considérese que la aplicación de gestión lee la entrada 46 en la secuencia de comandos 45 y el archivo 2F06 aún no existe. La aplicación de gestión utiliza la entrada 51 en la tabla 50 (con el identificador correspondiente 2F06) para crear el archivo requerido. La entrada 51 tiene los parámetros que se utilizarán al crear el archivo. La siguiente lista proporciona posibles parámetros de creación de archivos:

Tipo de archivo
ID de archivo
Nombre de archivo dedicado (DF) (identificador de aplicación (AID)) para la creación de ADF
Ciclo de vida
Condición de acceso remoto
Tamaño total de archivo
Condición de acceso
Datos de aplicación propietaria
Patrón de relleno

Los archivos se crean con una longitud fija y se inicializan con el patrón de relleno. El patrón de relleno es un patrón de datos que rellena inicialmente el archivo recién creado.

A continuación se describirá un segundo ejemplo de funcionamiento de la aplicación de gestión en la eUICC con referencia a la Figura 7.

En el bloque 111 se recibe una tabla de servicios. La tabla de servicios define qué servicio o servicios se requieren para proveer el perfil. La tabla de servicios se puede enviar en una secuencia de comandos antes de la secuencia de comandos principal para proveer un perfil. La secuencia de comandos de tabla de servicios contiene solo un comando, INSTALL INSTALL (instalar), que incluye la tabla de servicios en sus parámetros. Una tabla de servicios (ST) comprende una matriz de valores lógicos: verdadero o falso. Los servicios están numerados de 1 a n, por ejemplo. Si un servicio i está presente en el perfil asociado, entonces el valor de ST[i] se establece a verdadero. Un ejemplo de tabla de servicios puede adoptar la siguiente forma:

Servicio n.° 1:	Guía telefónica local
Servicio n.° 2:	Números de marcación fijos (FDN)
Servicio n.° 3:	Extensión 2
Servicio n.° 4:	Números de marcación de servicio (SDN)
Servicio n.° 5:	Extensión 3
Servicio n.° 6:	Números de marcación restringidos (BDN)
Servicio n.° 7:	Extensión 4
Servicio n.° 8:	Información de llamadas salientes (OCI y OCT)
Servicio n.° 9:	Información de llamadas entrantes (ICI e ICT)
Servicio n.° 10:	Almacenamiento de mensajes cortos (SMS)
Servicio n.° 11:	Informes de estado de mensajes cortos (SMSR)
Servicio n.° 12:	Parámetros del servicio de mensajes cortos (SMSP)
Servicio n.° 13:	Aviso de tarificación (AoC)
Servicio n.° 14:	Segundos parámetros de configuración de capacidad (CCP2)
Servicio n.° 15:	Identificador de mensaje de radiodifusión de célula
Servicio n.° 16:	Intervalos de identificadores de mensajes de radiodifusión de célula
Servicio n.° 17:	Nivel 1 de identificador de grupo
Servicio n.° 18:	Nivel 2 de identificador de grupo
Servicio n.° 19:	Nombre del proveedor de servicios

Servicio n.° 20: Selector de PLMN controlado por el usuario con tecnología de acceso
Servicio n.° 21: MSISDN
Servicio n.° 22: Imagen (IMG)
Servicio n.° 23: Soporte de áreas de servicio localizadas (SoLSA)
Servicio n.° 24: Servicio mejorado de precedencia y preferencia multinivel
Servicio n.° 25: Respuesta automática para eMLPP
Servicio n.° 26: RFU
Servicio n.° 27: Acceso GSM
Servicio n.° 28: Descarga de datos mediante SMS-PP
Servicio n.° 29: Descarga de datos mediante SMS-CB
Servicio n.° 30: Control de llamadas por USIM
Servicio n.° 31: Control MO-SMS por USIM
Servicio n.° 32: comando RUN AT COMMAND (ejecutar con comando)
Servicio n.° 33: se establecerá en "1"
Servicio n.° 34: Tabla de servicios habilitados
Servicio n.° 35: Lista de control APN (ACL)
Servicio n.° 36: Claves de control de despersonalización
Servicio n.° 37: Lista de redes que actúan conjuntamente
Servicio n.° 38: Contexto de seguridad GSM
Servicio n.° 39: Información CPBCCH
Servicio n.° 40: Exploración de investigación
Servicio n.° 41: MexE

…

Por ejemplo, si el número de servicio 19 está presente (nombre de proveedor de servicios), se creará el archivo EFspn.

En el bloque 112, la aplicación de gestión de la eUICC crea archivos obligatorios. Los archivos obligatorios son independientes de cualquier servicio particular y son necesarios para cualquier perfil creado. La Figura 8 muestra un ejemplo de una tabla FP 60 que incluye propiedades de archivo para archivos obligatorios y archivos opcionales. Los archivos obligatorios se indican mediante un número de servicio (n.º de servicio) = 0. La aplicación de gestión utiliza la tabla FP para crear los archivos obligatorios, buscando servicios con n.º de servicio = 0.

Además de los archivos obligatorios requeridos por cada perfil, algunos servicios requieren uno o más archivos adicionales. La aplicación de gestión en la eUICC implementa una estructura de datos, FP 60, que almacena, para cada servicio, los parámetros necesarios para crear estos archivos adicionales. Estos parámetros incluyen al menos: identidad de archivo, derechos de acceso y tamaño. La tabla FP incluye un valor de número de servicio (n.º de servicio) por entrada. Pueden guardarse, por ejemplo, en registros de longitud variable, con un registro para cada servicio. Cada registro contiene las identidades y parámetros de todos los archivos requeridos para un servicio dado. De manera alternativa, la tabla FP 60 puede contener múltiples registros por servicio, donde cada registro está identificado por el mismo valor de n.º de servicio. El orden de los bloques 111 y 112 puede invertirse. En el bloque 113 se lee la tabla de servicios recibida en el bloque 111. En el bloque 114, los archivos opcionales se crean explorando la tabla de servicios y creando una matriz:

```
para i = 1 a n
    si ST[i]
    crear archivos para todos los registros en FP donde el n.º de servicio = i;
```

Después del bloque 114, la aplicación de gestión en la eUICC ha creado ahora todos, o la mayoría de, los archivos que se requieren para proveer un perfil. En el bloque 115 se recibe una secuencia de comandos en la eUICC. La secuencia de comandos puede tener la misma forma que la mostrada en la Figura 4, es decir, con entradas CREATE FILE reemplazadas por entradas SELECT FILE. La secuencia de comandos puede recibirse antes de lo que se muestra en la Figura 7, tal como antes del bloque 111, o en cualquier punto antes de que se ejecute la secuencia de comandos. En el bloque 116 se ejecuta la secuencia de comandos principal. Haciendo de nuevo referencia a la secuencia de comandos de la Figura 4, considérese que la aplicación de gestión lee la entrada 46 en la secuencia de comandos 45. La entrada 46 se refiere a un archivo con el identificador 2F06. El archivo con identificador 2F06 ya se habrá creado mediante el proceso anterior en el bloque 112 o 114 usando la tabla de propiedades de archivo 50.

Cabe destacar que en cualquiera de los ejemplos descritos anteriormente, la secuencia de comandos 45 puede incluir al menos un comando de creación de archivo. Por ejemplo, puede ser necesario crear un archivo propietario cuya existencia no se pueda deducir o bien a partir de las normas o bien a partir de la tabla de servicios, y que todavía es necesario definir explícitamente en la secuencia de comandos enviada a la eUICC.

Las siguientes especificaciones definen los archivos requeridos durante el proceso de aprovisionamiento:

- para un USIM (SIM del Sistema Universal de Telecomunicaciones Móviles, UMTS): 3GPP 31.102
- para un SIM (módulo de identidad de abonado): 3GPP 51.011
- para un iSIM (SIM del subsistema multimedia IP, IMS): 3GPP 31.103
- para un CSIM (SIM de CDMA): 3GPP2 C.S0065-0

Usando estas especificaciones, es posible definir una lista de archivos obligatorios para un perfil dado y rellenar la estructura de datos FP 50, 60.

Utilizando la tabla de servicios y la especificación adecuada, es posible completar la lista de archivos obligatorios con los archivos opcionales (opcionales desde el punto de vista de la especificación) que se necesitan para implementar todos los servicios ofrecidos por cada una de las aplicaciones de acceso a red incluidas en el perfil.

En el ejemplo descrito anteriormente, las propiedades de archivos obligatorios y de archivos opcionales se almacenan juntos en una estructura de datos FP. Las entradas en la estructura de datos tienen un campo de n.º de servicio. Un valor del n.º de servicio = (1...n) indica un archivo opcional asociado a ese servicio. Un valor del n.º de servicio = 0 indica un archivo obligatorio. Un archivo obligatorio puede indicarse mediante cualquier otro valor adecuado de n.º de servicio, tal como un valor negativo (por ejemplo -1) o cualquier valor positivo fuera del intervalo esperado (1...n) utilizado en la tabla de servicios. Una alternativa al almacenamiento de propiedades de archivo en una única estructura de datos es almacenar una estructura de datos para archivos obligatorios y almacenar una estructura de datos aparte para archivos opcionales.

La Figura 9 muestra un procedimiento realizado en una entidad de envío, tal como la SM-DP 10. La SM-DP sabe que la eUICC tiene un almacenamiento local de datos de propiedad de archivo que permitirá que la eUICC cree ciertos archivos. El procedimiento comprende un bloque 120 para preparar una secuencia de comandos para proveer de forma remota un perfil en un elemento de seguridad. Se creará una secuencia de comandos a partir de un archivo de especificación que define las acciones que debe realizar la secuencia de comandos. De manera alternativa, el procedimiento se puede realizar para procesar o "filtrar" una secuencia de comandos existente. Al procesar la secuencia de comandos existente, el procedimiento puede reducir la longitud de la secuencia de comandos. La secuencia de comandos existente puede adoptar la forma de la secuencia de comandos mostrada en la Figura 3, que tiene comandos de creación de archivos. La Figura 9 muestra detalles adicionales del bloque 120 para el caso en que se procesa una secuencia de comandos existente. El bloque 121 recibe una secuencia de comandos para proveer un perfil. La secuencia de comandos puede ser una secuencia de comandos convencional que incluye comandos de creación de archivos. El bloque 122 identifica una primera entrada en la secuencia de comandos que comprende un comando para crear un archivo, donde el archivo corresponde a un archivo guardado en el almacenamiento local de datos de propiedad de archivo en el elemento de seguridad. El bloque 123 reemplaza la primera entrada en la secuencia de comandos por una segunda entrada en la secuencia de comandos. La segunda entrada es más corta que la primera entrada y carece del comando para crear el archivo. Tal como se describió anteriormente, la segunda entrada puede comprender un comando SELECT FILE. Esto mantiene la compatibilidad con una secuencia de comandos convencional al tiempo que reduce el tamaño de la secuencia de comandos. El bloque 124 proporciona una secuencia de comandos modificada que tiene una longitud más corta en comparación con la secuencia de comandos recibida en el bloque 121. El bloque 125 envía la secuencia de comandos al elemento de seguridad. Tal como se muestra en la Figura 2, la trayectoria hacia el elemento de seguridad puede incluir una SM-SR 12.

En los ejemplos descritos anteriormente, un comando CREATE FILE se reemplaza con un comando SELECT FILE. En otros ejemplos, un comando CREATE FILE puede reemplazarse por un comando diferente. Esto puede ser un comando propietario o un valor reservado, que es reconocible por la eUICC. De manera ventajosa, los comandos utilizados en la secuencia de comandos modificada son compatibles con ISO 7816.

La Figura 10 muestra un ejemplo de una eUICC 30. La eUICC 30 comprende un chip (circuito integrado) que tiene un procesador (CPU) 31 y almacenamiento. El almacenamiento puede comprender memoria de solo lectura (ROM) 32, memoria de acceso aleatorio (RAM) 33 y memoria reescribible no volátil 34, tal como memoria flash. Uno o más buses 36 acoplan de manera comunicativa unidades funcionales 31-35 de la eUICC.

El procesador 31 puede ser un microcontrolador, microprocesador o cualquier otro tipo adecuado de procesador para ejecutar instrucciones. Las instrucciones ejecutables por procesador 37 se pueden almacenar en la ROM 32 y/o la memoria flash 34. Las instrucciones ejecutables por procesador 37 pueden incluir una aplicación de gestión para proporcionar de forma remota un perfil. Una interfaz 35 admite la comunicación entre el dispositivo 30 y el dispositivo anfitrión 20. La memoria 34, o ROM 32, puede almacenar datos de propiedad de archivo 50 que se utilizan para crear localmente archivos en el elemento de seguridad.

Modificaciones y otras formas de realización de la invención divulgada serán concebidas por un experto en la técnica que tenga el beneficio de las enseñanzas presentadas en las descripciones anteriores y los dibujos asociados. Por lo tanto, debe entenderse que la invención no debe limitarse a las formas de realización específicas divulgadas y que las modificaciones y otras formas de realización están incluidas dentro del alcance de esta divulgación. Aunque en el presente documento se pueden emplear términos específicos, se utilizan únicamente en un sentido genérico y descriptivo y no con fines limitativos.

REIVINDICACIONES

1. Un procedimiento para preparar una secuencia de comandos APDU ISO 7816 que enviar a un elemento de seguridad (30) para proveer de forma remota un perfil (31) en el elemento de seguridad (30), en el que:

el elemento de seguridad (30) tiene un almacenamiento local de datos de propiedad de archivo (50) correspondientes a parámetros para un comando de creación de archivo,

comprendiendo el procedimiento:

recibir (121) una primera secuencia de comandos que comprende un comando de creación de archivo;
determinar (122) si el comando de creación de archivo corresponde a un archivo cuyas propiedades de archivo están almacenadas en el almacenamiento local de datos de propiedad de archivo en el elemento de seguridad;
si el comando de creación de archivo corresponde al archivo cuyas propiedades de archivo están almacenadas, reemplazar (123) el comando de creación de archivo por un comando de selección de archivo para generar una secuencia de comandos modificada; y
proporcionar (124) la secuencia de comandos modificada.

2. Un procedimiento para proveer un perfil en un elemento de seguridad (30), que comprende:

recibir (101) una secuencia de comandos APDU ISO 7816 para proveer el perfil;
recibir una tabla de servicio que indica al menos un servicio requerido por el perfil, y donde el almacenamiento local de datos de propiedad de archivo incluye una indicación de un servicio al que están asociados los datos de propiedad de archivo;
ejecutar (102) mediante una aplicación de gestión la secuencia de comandos para proveer el perfil, donde la ejecución mediante la aplicación de gestión comprende:
leer (103) un comando de selección de archivo en la secuencia de comandos;
determinar (104) si existe el archivo; y, si el archivo no existe, crear (105) el archivo usando un almacenamiento local de datos de propiedad de archivo correspondientes a parámetros de un comando de creación de archivo en el elemento de seguridad;

donde el procedimiento comprende además:

utilizar la tabla de servicios para identificar los servicios requeridos para el perfil;
recuperar datos de propiedad de archivo del almacenamiento local de datos de propiedad de archivo para cada servicio requerido; y
crear al menos un archivo para el servicio requerido usando los datos de propiedad de archivo recuperados.

3. Un procedimiento de acuerdo con la reivindicación 2, en el que el comando de selección de archivo en la secuencia de comandos comprende un identificador de archivo y el procedimiento comprende:

usar el identificador de archivo para localizar datos de propiedad de archivo en el almacenamiento local; y
crear el archivo con el identificador y los datos de propiedad de archivo.

4. Un procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que los datos de propiedad de archivo comprenden al menos uno de: un identificador de archivo, un tamaño de archivo y derechos de acceso a archivo.

5. Un procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en el que el elemento de seguridad es una tarjeta de circuito integrado universal incrustada.

6. Un elemento de seguridad, que comprende un procesador y una memoria, donde la memoria contiene instrucciones ejecutables por el procesador, mediante las cuales el procesador está configurado para realizar el procedimiento de acuerdo con una cualquiera de las reivindicaciones 2 a 4.

7. Un elemento de seguridad de acuerdo con la reivindicación 6, donde el elemento de seguridad es una tarjeta de circuito integrado universal incrustada.

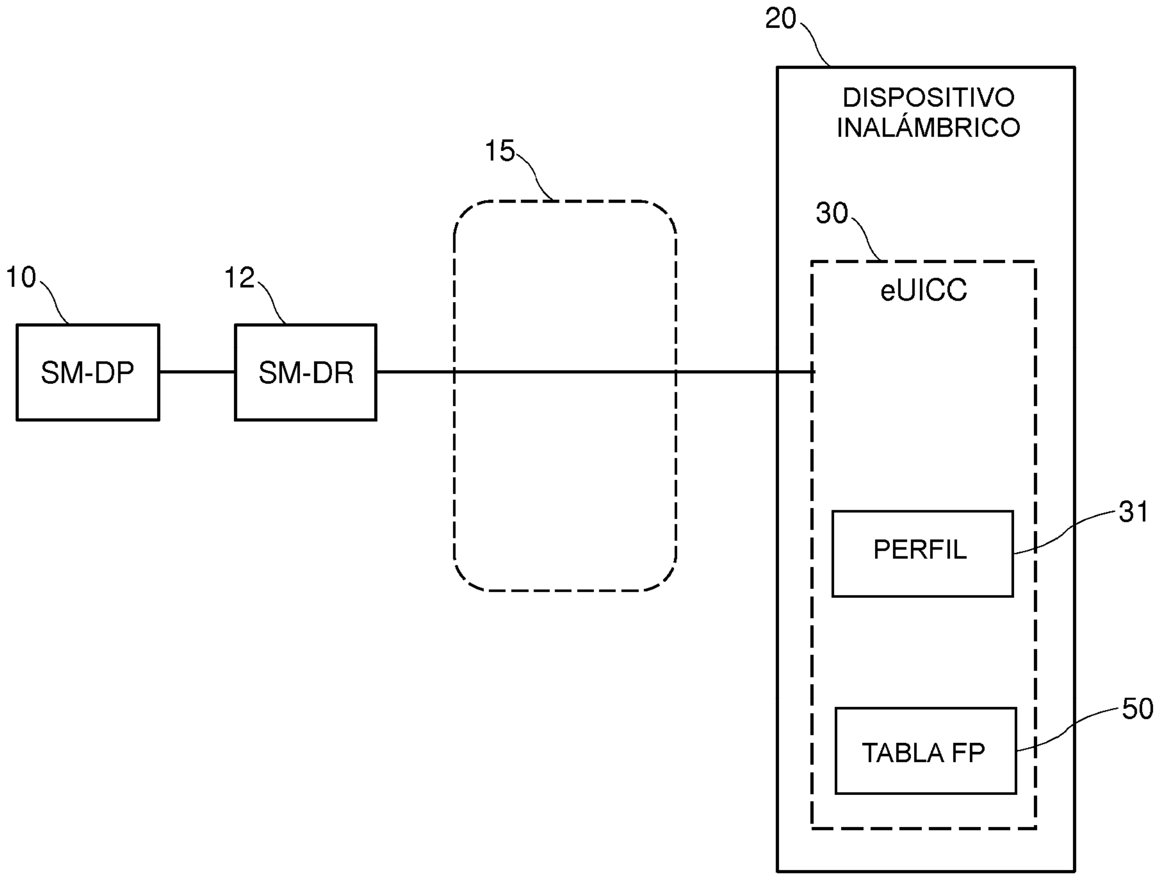
20
DISPOSITIVO
INALÁMBRICO
15
30
eUICC
10
12
SM-DP
SM-DR
PERFIL
31
TABLA FP
50

Fig. 1

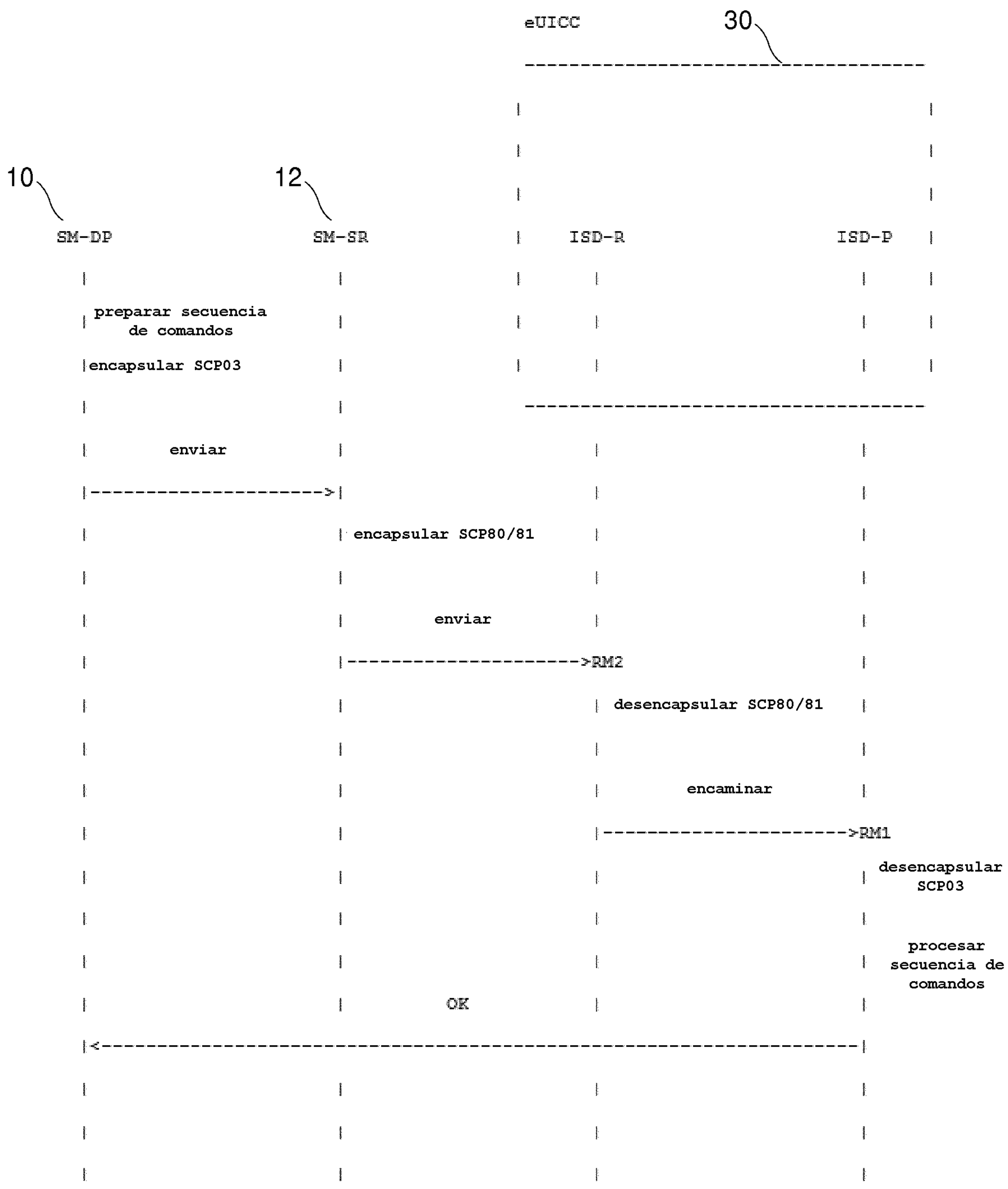
eUICC
30
10
12
SM-DP
SM-SR
ISD-R
ISD-P
preparar secuencia de comandos
encapsular SCP03
enviar
encapsular SCP80/81
enviar
RM2
desencapsular SCP80/81
encaminar
RM1
desencapsular SCP03
procesar secuencia de comandos
OK

Fig. 2

40

Secuencia de comandos antes:

```
...
CREATE FILE 000127001100103F00100000000001000000000000000002F060102000000000000000000000400010000 (9000)
CREATE FILE FF0028000A00152F060106000000010000000030000000 2F060101000000000000000000580017F90000000 (9000)
UPDATE RECORD 01043080017F90008401D490008C02A0E89000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF (9000)
UPDATE RECORD 02043080017F90008401D490008C02A0E89000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF (9000)
UPDATE RECORD 03043080017F90008401D490008C02A0E89000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF (9000)
UPDATE RECORD 04043080017F90008401D490008C02A0E89000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF (9000)
UPDATE RECORD 05043080017F90008401D490008C02A0E89000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF (9000)
CREATE FILE 00012300030005220D010000000001000000001000000002F0601030000000000000000000000 (9000)
APPEND RECORD 00001003933F57845F7069213380FFFFFF5256 (9000)
CREATE FILE FF002300050004220F010000000001000000008000000002F0601040000000000000000000000 (9000)
UPDATE RECORD 0104080000000000000000 (9000)
```

41

42

43

Fig. 3

45

Secuencia de comandos después:

```
<La cabecera de la secuencia de comandos va aquí>
...
SELECT FILE 2F06
UPDATE RECORD 01043080017F90008401D490008C02A0E89000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF (9000)
UPDATE RECORD 02043080017F90008401D490008C02A0E89000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF (9000)
UPDATE RECORD 03043080017F90008401D490008C02A0E89000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF (9000)
UPDATE RECORD 04043080017F90008401D490008C02A0E89000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF (9000)
UPDATE RECORD 05043080017F90008401D490008C02A0E89000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF (9000)
SELECT FILE 220D
APPEND RECORD 00001003933F57845F7069213380FFFFFF5256 (9000)
SELECT FILE 220F
UPDATE RECORD 0104080000000000000000 (9000)
```

46

47

48

Fig. 4

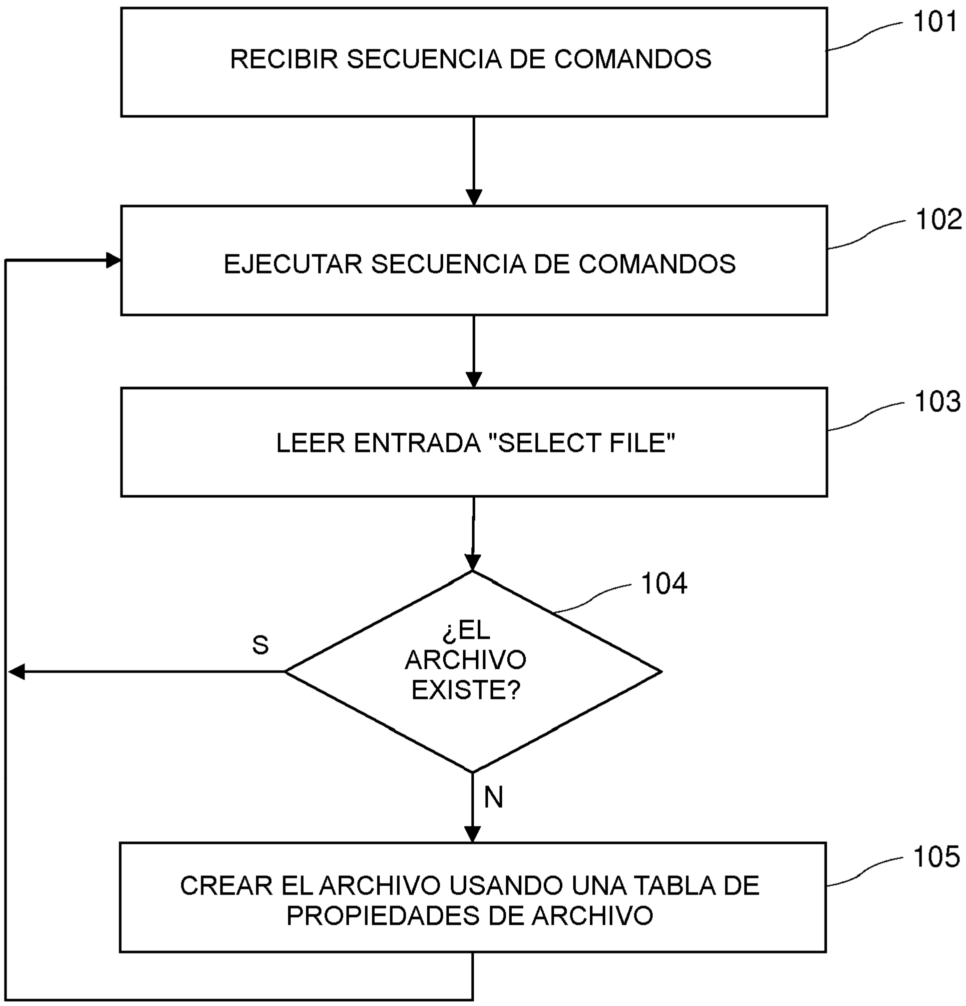
RECIBIR SECUENCIA DE COMANDOS
101
EJECUTAR SECUENCIA DE COMANDOS
102
LEER ENTRADA "SELECT FILE"
103
¿EL ARCHIVO EXISTE?
104
S
N
CREAR EL ARCHIVO USANDO UNA TABLA DE PROPIEDADES DE ARCHIVO
105

Fig. 5

50

Tabla FP

	FID	Parámetros
51	2F06	000127001100103F001000000000001000000000000000002F060102000000000000000000000400010000
52	220D	FF0028000A00152F0601060000000010000000003000000002F06010100000000000000000580017F90000000
53	220F	FF00230005000422OF0100000000001000000000800000002F060104000000000000000000000000

Fig. 6

60

Tabla FP

FID	Parámetros	N.° de servicio
2F06	000127001100103F001000000000001000000000000000002F060102000000000000000000000400010000	0
220D	FF0028000A00152F0601060000000010000000003000000002F06010100000000000000000580017F90000000	0
220F	FF00230005000422OF0100000000001000000000800000002F060104000000000000000000000000	0

****	*********	1
****	*******	2
****	*******	3
****	*********	4

Fig. 8

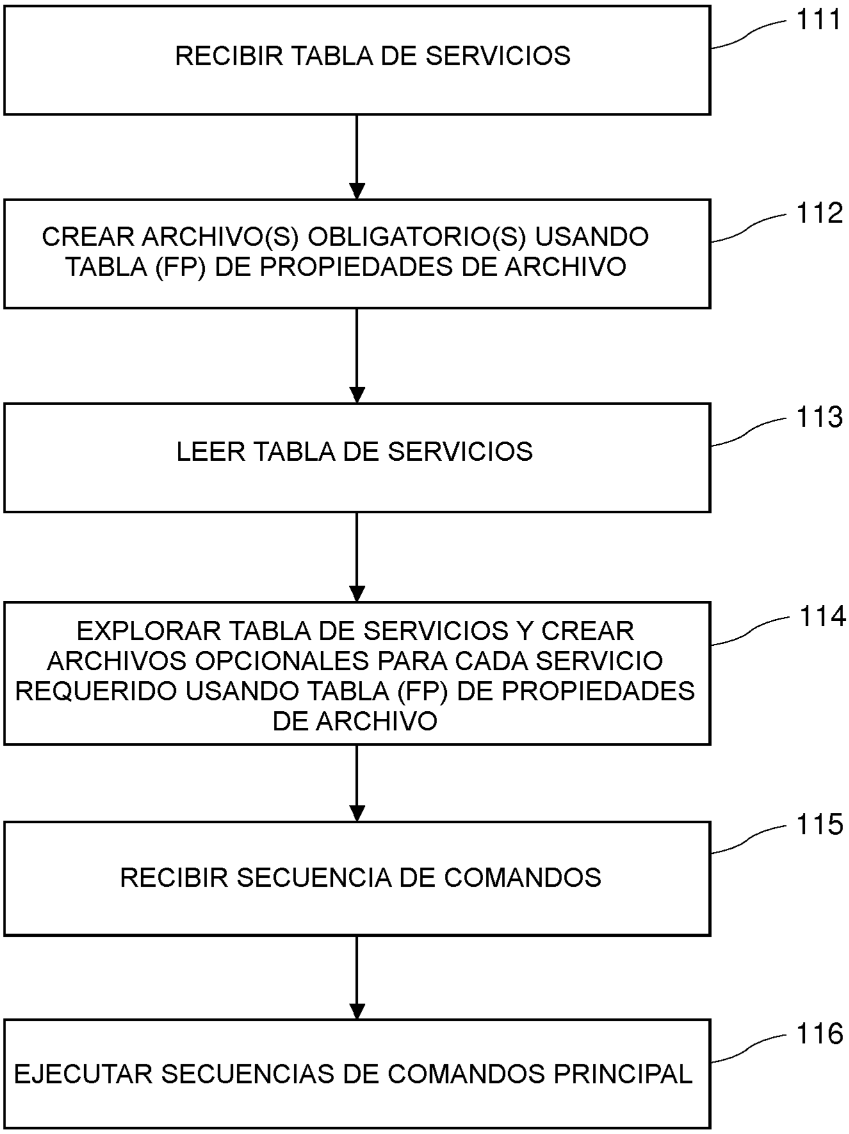
RECIBIR TABLA DE SERVICIOS
111
CREAR ARCHIVO(S) OBLIGATORIO(S) USANDO TABLA (FP) DE PROPIEDADES DE ARCHIVO
112
LEER TABLA DE SERVICIOS
113
EXPLORAR TABLA DE SERVICIOS Y CREAR ARCHIVOS OPCIONALES PARA CADA SERVICIO REQUERIDO USANDO TABLA (FP) DE PROPIEDADES DE ARCHIVO
114
RECIBIR SECUENCIA DE COMANDOS
115
EJECUTAR SECUENCIAS DE COMANDOS PRINCIPAL
116

Fig. 7

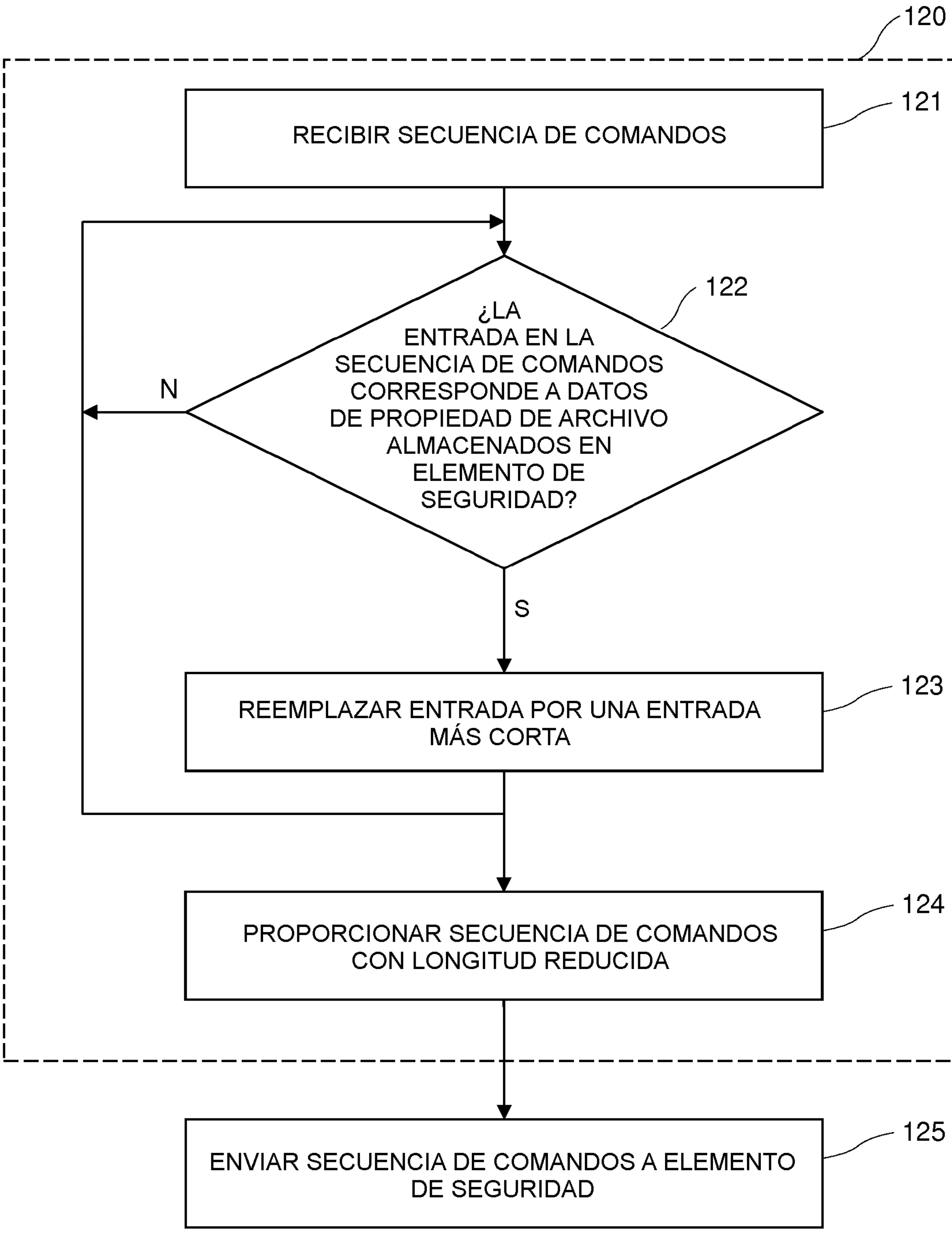
120
RECIBIR SECUENCIA DE COMANDOS
121
¿LA ENTRADA EN LA SECUENCIA DE COMANDOS CORRESPONDE A DATOS DE PROPIEDAD DE ARCHIVO ALMACENADOS EN ELEMENTO DE SEGURIDAD?
122
N
S
REEMPLAZAR ENTRADA POR UNA ENTRADA MÁS CORTA
123
PROPORCIONAR SECUENCIA DE COMANDOS CON LONGITUD REDUCIDA
124
ENVIAR SECUENCIA DE COMANDOS A ELEMENTO DE SEGURIDAD
125

Fig. 9

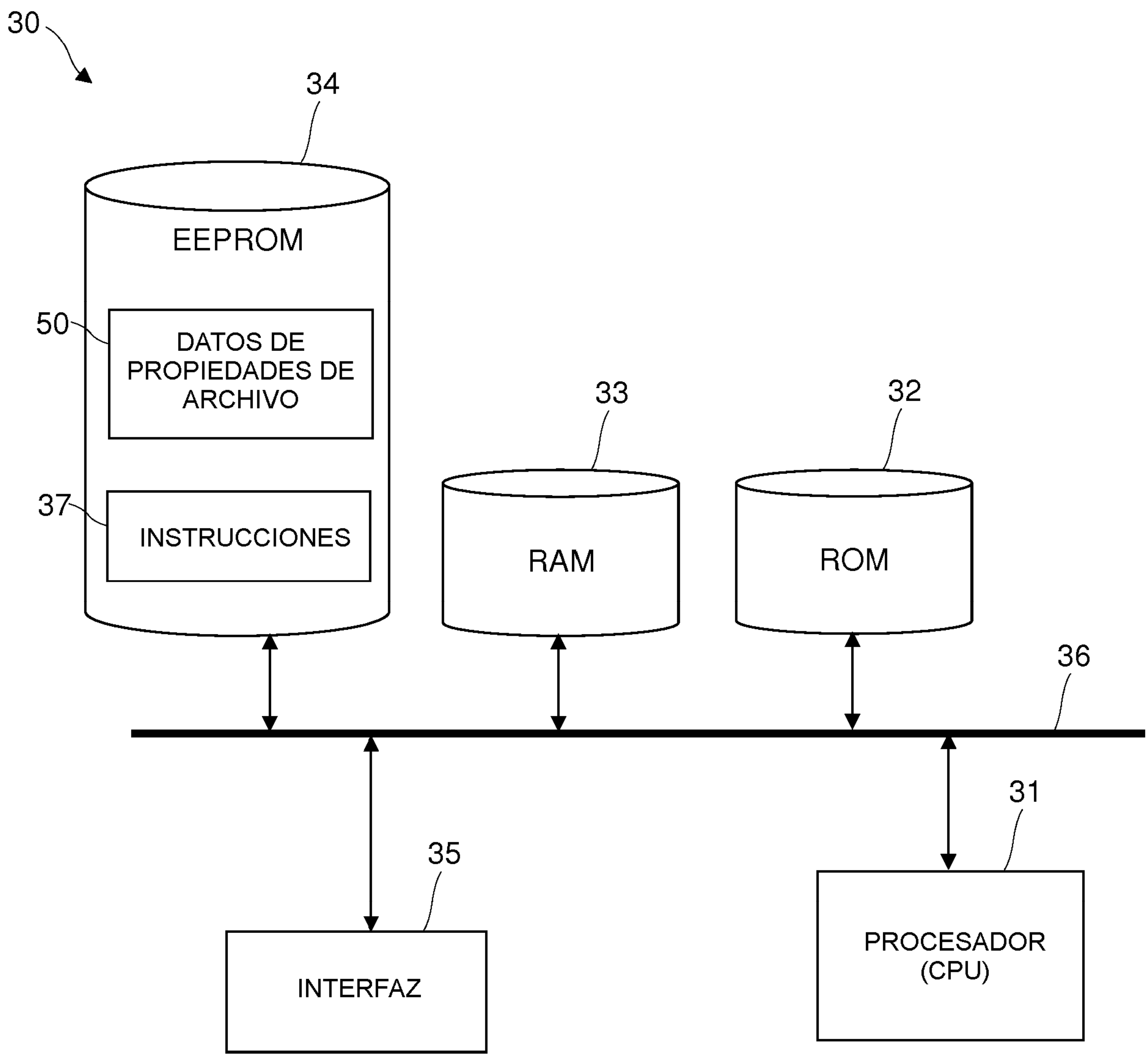
30
34
EEPROM
50
DATOS DE PROPIEDADES DE ARCHIVO
37
INSTRUCCIONES
33
RAM
32
ROM
36
31
35
INTERFAZ
PROCESADOR (CPU)

Fig. 10