(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 700 589**

(51) Int. CI.:

H04W 12/02 (2009.01)
H04W 4/00 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.09.2015 PCT/EP2015/070765**

(87) Fecha y número de publicación internacional: **28.04.2016 WO16062452**

(96) Fecha de presentación y número de la solicitud europea: **10.09.2015 E 15763879 (2)**

(97) Fecha y número de publicación de la concesión europea: **04.07.2018 EP 3210403**

(54) Título: **Método de transmisión de datos desde un dispositivo electrónico seguro a un servidor**

(30) Prioridad:

23.10.2014 EP 14306684

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.02.2019

(73) Titular/es:

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

(72) Inventor/es:

BERARD, XAVIER y
GALLAND, ANTOINE

(74) Agente/Representante:

CASANOVAS CASSA, Buenaventura

DESCRIPCION

Método de transmisión de datos desde un dispositivo electrónico seguro a un servidor

(Campo de la invención)

La presente invención se refiere a métodos de envío de datos desde un dispositivo electrónico seguro a un servidor remoto. Se refiere particularmente a métodos para enviar de forma segura una respuesta correspondiente a un comando iniciado por un servidor aplicativo.

(Antecedentes de la invención)

Un dispositivo electrónico seguro es un componente inviolable capaz de almacenar datos y proporcionar servicios de manera segura. En general, un dispositivo electrónico seguro es un componente físico que tiene una cantidad limitada de memoria, un procesador con capacidades limitadas y que está desprovisto de batería. Por ejemplo, una UICC (Tarjeta Universal de Circuito Integrado) es un dispositivo electrónico seguro que integra aplicaciones SIM/USIM para fines de telecomunicaciones. Un dispositivo electrónico seguro se puede instalar, de forma fija o no, en un terminal, como un teléfono móvil por ejemplo. En algunos casos, los terminales están constituidos por máquinas que se comunican con otras máquinas para aplicaciones M2M (Machine to Machine).

Un dispositivo electrónico seguro puede tener el formato de una tarjeta inteligente. Un dispositivo electrónico seguro puede ser un chip soldado a la placa madre del dispositivo huésped y constituye un elemento seguro integrado (eSE).

Un dispositivo electrónico seguro puede contener varias UICC emuladas.

Un dispositivo electrónico seguro puede comprender una aplicación destinada a comunicarse con un servidor aplicativo remoto. La mayoría de las soluciones de telecomunicaciones dependen de un protocolo de comunicación basado en un comando/respuesta entre un servidor aplicativo y una aplicación integrada en un dispositivo electrónico seguro. Este protocolo está mapeado en un Paquete de Comandos seguro en un SM (mensaje corto) MT (móvil terminado) y un paquete de respuesta segura en un SM MO (móvil originado) para la comunicación. Tal diseño puede beneficiarse de la capa de seguridad del canal de comunicación del operador de telecomunicaciones para que el servidor aplicativo envíe un comando y para que la aplicación en el dispositivo electrónico envíe una respuesta. Los dispositivos electrónicos seguros involucrados en esta invención pueden utilizar dicho canal de comunicación seguro.

De acuerdo con ETSI TS 143.019 V6.0.0, las respuestas son gestionadas por un controlador especializado, denominado EnvelopeResponseHandler, en la UICC.

El ETSI TS 102 223 describe el principio de una sesión proactiva que permite a una UICC enviar comandos proactivos a su dispositivo huésped. Los comandos proactivos se gestionan en la UICC a través de un controlador específico llamado ProactiveHandler.

Desafortunadamente, según el §6.6 del ETSI TS 143.019 V6.0.0, el EnvelopeResponseHandler ya no se encuentra disponible tras la primera invocación del ProactiveHandler. Por lo tanto, cuando el servidor aplicativo envía un comando solicitando la apertura de una sesión proactiva, el dispositivo electrónico no puede enviar su respuesta como de costumbre.

Existe la necesidad de proporcionar una solución que permita que un dispositivo electrónico seguro envíe una respuesta al servidor aplicativo de manera segura tras una invocación del ProactiveHandler.

(Sumario de la invención)

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

El objeto de la presente invención es un método para gestionar una respuesta generada por una aplicación que está incorporada en un dispositivo electrónico seguro que actúa como una UICC en respuesta a un primer comando que solicita la apertura de una sesión proactiva. Un servidor aplicativo cuenta con un servidor OTA para enviar el primer comando al dispositivo electrónico. El primer comando está protegido con una capa de seguridad por el servidor OTA. El método comprende los pasos de:

- el servidor aplicativo envía un segundo comando al dispositivo electrónico seguro, solicitando dicho segundo comando el envío de dicha respuesta y encontrándose protegido por la capa de seguridad proporcionada por el servidor OTA,
- en respuesta al segundo comando, el dispositivo electrónico seguro confecciona un paquete de respuesta segura que comprende la respuesta protegida con la capa de seguridad proporcionada por el servidor OTA y

envía el paquete de respuesta segura al servidor OTA quien, a su vez, envía la respuesta al servidor aplicativo.

Ventajosamente, el dispositivo electrónico seguro puede enviar al servidor aplicativo una respuesta intermedia a dicho primer comando, comprendiendo dicha respuesta intermedia una petición de extensión de tiempo y estando protegida dicha respuesta intermedia con la capa de seguridad proporcionada por el servidor OTA.

Ventajosamente, la petición puede comprender una extensión de tiempo expresada como una duración fijada, una duración indefinida o el acaecimiento de un evento especificado.

Ventajosamente, el dispositivo electrónico seguro puede enviar al servidor aplicativo un mensaje indicando que la respuesta puede ser recuperada.

Ventajosamente, el mensaje puede ser enviado directamente al servidor aplicativo sin utilizar la capa de seguridad proporcionada por el servidor OTA.

Otro objeto de la presente invención es un dispositivo electrónico seguro que actúa como una UICC y que incluye una aplicación capaz de ejecutar un primer comando que solicita la apertura de una sesión proactiva. El primer comando es iniciado por un servidor aplicativo y protegido con una capa de seguridad proporcionada por un servidor OTA. La aplicación está configurada para generar una respuesta correspondiente con el primer comando. El dispositivo electrónico seguro está configurado para gestionar un segundo comando que solicita el envío de la respuesta. El dispositivo electrónico seguro está configurado para confeccionar un paquete de respuesta segura que comprende la respuesta protegida con la capa de seguridad proporcionada por el servidor OTA y para enviar el paquete de respuesta segura al servidor OTA en respuesta al segundo comando.

Ventajosamente, el dispositivo electrónico seguro puede estar configurado para enviar al servidor aplicativo una respuesta intermedia a dicho primer comando, comprendiendo dicha respuesta intermedia una petición de extensión de tiempo, estando protegida dicha respuesta intermedia con la capa de seguridad proporcionada por el servidor OTA.

Ventajosamente, el dispositivo electrónico seguro puede ser configurado para enviar al servidor aplicativo un mensaje indicando que la respuesta puede ser recuperada.

Otro objeto de la presente invención es un sistema que incluye un servidor aplicativo y un dispositivo electrónico seguro de acuerdo con la invención, en el que el servidor aplicativo está configurado para enviar el segundo comando después de un evento y para obtener la respuesta del servidor OTA en respuesta al envío del segundo comando.

Ventajosamente, el evento se puede seleccionar de entre un conjunto que comprende la recepción de un mensaje indicando que la respuesta puede ser recuperada, una duración específica después de la recepción de una petición de extensión de tiempo por la parte del servidor aplicativo y una duración predefinida después del envío del primer comando.

(Breve descripción de los dibujos)

Otras características y ventajas de la presente invención surgirán más claramente a partir de una lectura de la siguiente descripción de varias realizaciones preferidas de la invención con referencia a los correspondientes dibujos adjuntos en los que:

- La Figura 1 representa un primer ejemplo de intercambio de mensajes entre un servidor aplicativo y un applet (es decir, una aplicación) incorporado en un dispositivo electrónico seguro según el estado la técnica anterior;
- la Figura 2 representa un segundo ejemplo de intercambio de mensajes entre un servidor aplicativo y un applet incorporado en un dispositivo electrónico seguro según el estado de la técnica anterior; y
- La Figura 3 representa un ejemplo de intercambio de mensajes entre un servidor aplicativo y un applet incorporado en un dispositivo electrónico según la invención.

(Descripción detallada de las realizaciones preferidas)

La invención puede aplicarse a cualquier tipo de dispositivo electrónico seguro configurado para actuar como una UICC. Por ejemplo, el dispositivo electrónico seguro puede ser una tarjeta inteligente, una UICC, una UICC integrada (eUICC), una SIM integrada o una UICC implementada por software.

El dispositivo electrónico seguro se puede acoplar a cualquier tipo de máquina huésped que tenga una banda base y que pueda establecer una sesión de comunicación con el dispositivo electrónico seguro. Por ejemplo, la máquina huésped puede ser un teléfono móvil, una tableta, un PC, un vehículo, un medidor, una máquina tragaperras, un televisor o un ordenador.

A modo de ilustración, la figura 1 muestra un primer ejemplo de intercambio de mensajes entre un servidor aplicativo SV0 y un applet A0 incorporado en un dispositivo electrónico seguro de acuerdo con la técnica anterior.

El mecanismo Over The Air (también conocido como OTA) se define, entre otros, por los estándares GSM 03.40, GSM 03.48 y ETSI/SCP-3GPP-3GPP2. Estos documentos detallan protocolos específicos y una capa de seguridad conocida como "capa de seguridad 03.48".

El servidor aplicativo SV0 envía un comando a través de un mensaje al servidor OTA SV2. Entonces, el servidor OTA SV2 compone un SM MT que contiene el mensaje. El servidor OTA SV2 protege el contenido de SM MT utilizando la capa de seguridad 03.48. Luego, el applet descifra el SM MT recibido, ejecuta el comando, genera una respuesta y proporciona la respuesta al EnvelopeResponseHandler. Entonces, el sistema operativo del dispositivo electrónico seguro crea un SM MO y lo envía al servidor OTA a través de la capa de seguridad 03.48. Luego, el servidor OTA descifra el SM MO, recupera la respuesta y envía la respuesta al servidor aplicativo SV0.

En el estado de la técnica, el envío del comando y su respuesta correspondiente están protegidos por la misma capa de seguridad.

La figura 2 muestra un segundo ejemplo de intercambio de mensajes entre el servidor aplicativo SV0 y el applet A0 incorporado en un dispositivo electrónico seguro de acuerdo con la técnica anterior.

En este ejemplo, el comando iniciado por el servidor aplicativo SV0 solicita al applet A0 que abra una sesión proactiva. El comando se envía desde el servidor aplicativo SV0 al applet A0 de manera similar al ejemplo de la Figura 1. Por ejemplo, la sesión proactiva puede esperar los datos seleccionados por el usuario del teléfono móvil que aloja el dispositivo electrónico seguro. Cuando el applet A0 debe enviar la respuesta correspondiente al comando recibido, la capa de seguridad 03.48 ya no está disponible. El contenido del EnvelopeResponseHandler debe ser enviado antes de la primera invocación de un método ProactiveHandler.send o antes de la finalización de processToolkit, de modo que el Applet pueda ofrecer estos datos al equipo móvil (p.ej. 9Fxx/9Exx/91xx). Después de la primera invocación del método ProactiveHandler.send, el EnvelopeResponseHandler ya no se encuentra disponible. El SM MO que contiene la respuesta no se puede transmitir de la misma manera que se envió en el ejemplo de la Figura 1. La línea de puntos muestra que el mensaje no puede ser enviado.

La figura 3 muestra un ejemplo de intercambio de mensajes entre un servidor aplicativo SV1 y un applet A1 incorporado en un dispositivo electrónico seguro de acuerdo con la invención.

En este ejemplo, el comando C1 iniciado por el servidor aplicativo SV1 solicita al applet A1 que abra una sesión proactiva. El comando C1 es enviado desde el servidor aplicativo SV1 al applet Al de una manera similar al ejemplo de la Figura 1. La sesión proactiva puede mostrar datos al usuario a través de la pantalla del teléfono móvil. Por ejemplo, se puede ejecutar el comando proactivo “Mostrar Texto”.

Una vez que el applet A1 ha iniciado la sesión proactiva, se cierra la sesión segura establecida entre el servidor OTA SV2 y el dispositivo electrónico seguro.

El applet genera una respuesta R1 correspondiente a la ejecución del comando C1.

Cuando acontece un evento EV, el servidor aplicativo SV1 envía otro comando C2 al dispositivo electrónico seguro TK. El comando C2 solicita el envío de la respuesta R1. El comando C2 está protegido por la capa de seguridad proporcionada por el servidor OTA SV2. En otras palabras, el servidor aplicativo SV1 envía el comando C2 al servidor OTA SV2, quien a su vez confecciona un SM MT que comprende el comando C2 y envía el SM MT al dispositivo electrónico seguro TK.

Entonces, el dispositivo electrónico seguro TK genera un paquete de respuesta segura R2S que comprende la respuesta R1 protegida con la capa de seguridad proporcionada por el servidor OTA SV2. Por ejemplo, el paquete de respuesta seguro R2S puede ser un SM MO protegido con el mecanismo de seguridad 0348.

Seguidamente, el paquete de respuesta segura R2S es enviado desde el dispositivo electrónico seguro al servidor OTA SV2, quien a su vez recupera la respuesta R1 del paquete de respuesta segura R2S y envía la respuesta R1 al servidor aplicativo SV1.

En este punto, el servidor aplicativo es capaz de asociar la respuesta R1 recibida con el primer comando C1.
Ventajosamente, el dispositivo electrónico seguro TK puede enviar una respuesta intermedia IR al servidor aplicativo SV1 para solicitar tiempo adicional antes de abrir la sesión proactiva. Tal como se muestra con la línea de puntos en la Figura 3, el envío de esta respuesta intermedia IR es opcional. Debido a que no se ha iniciado aun la sesión proactiva, la respuesta intermedia IR puede enviarse de forma segura a través del servidor OTA SV2 utilizando la capa de seguridad proporcionada por el servidor OTA SV2. La respuesta intermedia IR comprende una petición RQ de extensión de tiempo. La extensión de tiempo se puede expresar como una duración fijada por el dispositivo electrónico seguro TK, una duración que será determinada por el servidor aplicativo SV1 (por ejemplo, duración

indefinida) o el acaecimiento de un evento especificado. Por ejemplo, el evento especificado puede ser la recepción de un mensaje adicional indicando que la respuesta R1 puede ser recuperada del dispositivo electrónico seguro TK o el hecho de que se debe establecer una nueva sesión de comunicación con el dispositivo electrónico seguro TK por cualquier motivo.

Ventajosamente, el dispositivo electrónico seguro TK puede enviar un mensaje MG al servidor aplicativo SV1 para indicar que la respuesta R1 está disponible en el lado del dispositivo electrónico seguro y puede ser recuperado. Como se muestra en la línea de puntos en la Figura 3, el envío de este mensaje MG es opcional. Por ejemplo, el dispositivo electrónico seguro TK puede enviar directamente al servidor aplicativo SV1 el mensaje MG encapsulado en SM MO. En este caso, el mensaje MG no está protegido por la capa de seguridad proporcionada por el servidor OTA SV2. Al recibir el mensaje MG, el servidor aplicativo SV1 enviará el comando C2 de la manera que se describió anteriormente.

Una ventaja de la invención es reutilizar la capa de seguridad de ETSI TS 102 225 para el envío del comando aplicativo al dispositivo electrónico seguro. Permite aprovechar el mecanismo de mensajería segura ya diseñado para dispositivos electrónicos seguros que actúan como una UICC. En comparación con las aplicaciones existentes, la aplicación A1 no tiene que implementar una función adicional para gestionar su propia capa de seguridad.

La invención evita la gestión de un conjunto adicional de claves (para asegurar el envío de la respuesta R1) por parte del servidor aplicativo y una flota de dispositivos electrónicos seguros.

Debe entenderse, dentro del alcance de la invención, que las realizaciones descritas anteriormente se proporcionan como ejemplos no limitativos. En particular, el dispositivo electrónico seguro puede comprender cualquier cantidad de UICC virtual y la aplicación no ser necesariamente un applet.

REIVINDICACIONES

1. Un método para gestionar una respuesta (R1) generada por una aplicación (A1) incorporada en un dispositivo electrónico seguro (TK) que actúa como una UICC, en respuesta a un primer comando (C1) que solicita la apertura de una sesión proactiva, un servidor aplicativo (SV1) que cuenta con un servidor OTA (SV2) para enviar el primer comando (C1) al dispositivo electrónico seguro (TK), estando dicho primer comando (C1) protegido por una capa de seguridad proporcionada por el servidor OTA (SV2)0
caracterizado porque dicho método comprende los pasos:

- el servidor aplicativo (SV1) envía un segundo comando (C2) al dispositivo electrónico seguro (TK), solicitando dicho segundo comando (C2) el envío de dicha respuesta (R1) y encontrándose protegido por la capa de seguridad proporcionada por el Servidor OTA (SV2),
- en respuesta al segundo comando (C2), el dispositivo electrónico seguro (TK) confecciona un paquete de respuesta segura (R2S) que comprende la respuesta (R1) protegida por la capa de seguridad proporcionada por el servidor OTA (SV2) y envía el paquete de respuesta segura (R2S) al servidor OTA (SV2) quien, a su vez, envía la respuesta (R1) al servidor aplicativo (SV1).

2. Un método de acuerdo con la reivindicación 1, en el que el dispositivo electrónico seguro (TK) envía al servidor aplicativo (SV1) una respuesta intermedia (IR) a dicho primer comando (C1), comprendiendo dicha respuesta intermedia (IR) una solicitud (RQ) de extensión de tiempo, estando protegida dicha respuesta intermedia (IR) por la capa de seguridad proporcionada por el servidor OTA (SV2).

3. Un método de acuerdo con la reivindicación 2, en el que la solicitud (RQ) comprende una extensión de tiempo expresada como una duración fijada, una duración indefinida o el acaecimiento de un evento especificado.

4. Un método de acuerdo con la reivindicación 1, en el que el dispositivo electrónico seguro (TK) envía al servidor aplicativo (SV1) un mensaje (MG) indicando que la respuesta (R1) puede ser recuperada.

5. Un método de acuerdo con la reivindicación 4, en el que dicho mensaje (MG) es enviado directamente al servidor aplicativo (SV1) sin utilizar la capa de seguridad proporcionada por el servidor OTA (SV2).

6. Un dispositivo electrónico seguro (TK) que actúa como una UICC y que incluye una aplicación (A1) capaz de ejecutar un primer comando (C1) que solicita la apertura de una sesión proactiva, siendo iniciado dicho primer comando (C1) por un servidor aplicativo (SV1) y protegido con una capa de seguridad proporcionada por un servidor OTA (SV2), siendo la aplicación (A1) capaz de generar una respuesta (R1) correspondiente al primer comando (C1),
caracterizado porque el dispositivo electrónico seguro (TK) está configurado para controlar un segundo comando (C2) solicitando el envío de la respuesta (R1),
y **porque** el dispositivo electrónico seguro (TK) está configurado para confeccionar un paquete de respuesta segura (R2S) que comprende la respuesta (R1) protegida con la capa de seguridad proporcionada por el servidor OTA (SV2) y para enviar el paquete de respuesta segura (R2S) al servidor OTA (SV2) en respuesta al segundo comando (C2).

7. Un dispositivo electrónico seguro (TK) de acuerdo con la reivindicación 6, en el que el dispositivo electrónico seguro (TK) está configurado para enviar al servidor aplicativo (SV1) una respuesta intermedia (IR) a dicho primer comando (C1), comprendiendo dicha respuesta intermedia (IR) una solicitud (RQ) de extensión de tiempo, estando dicha respuesta intermedia (IR) protegida con la capa de seguridad proporcionada por el servidor OTA (SV2).

8. Un dispositivo electrónico seguro (TK) de acuerdo con la reivindicación 6, en el que el dispositivo electrónico seguro (TK) está configurado para enviar al servidor aplicativo (SV1) un mensaje (MG) indicando que la respuesta (R1) puede ser recuperada.

9. Un **sistema** que incluye un servidor aplicativo (SV1) y un dispositivo electrónico seguro (TK) de acuerdo con la reivindicación 6, en el que el servidor aplicativo (SV1) está configurado para enviar el segundo comando (C2) después de un evento (EV) y para obtener la respuesta (R1) del servidor OTA (SV2) en contestación al envío del segundo comando (C2).

10. Un sistema de acuerdo con la reivindicación 8, en el que el evento (EV) se selecciona de entre un conjunto que comprende la recepción de un mensaje (MG) indicando que la respuesta (R1) puede ser recuperada, una duración específica tras la recepción de una solicitud (RQ) de extensión de tiempo y una duración predefinida después del envío del primer comando (C1).

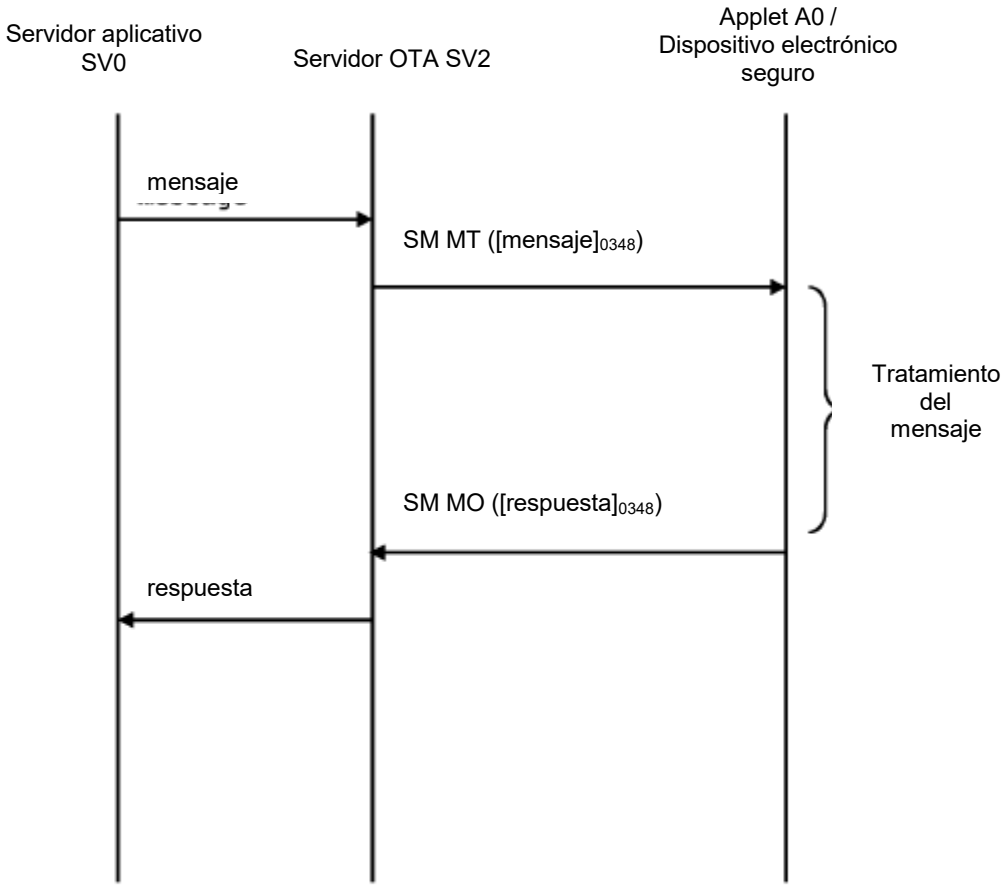

FIG. 1

(Arte anterior)

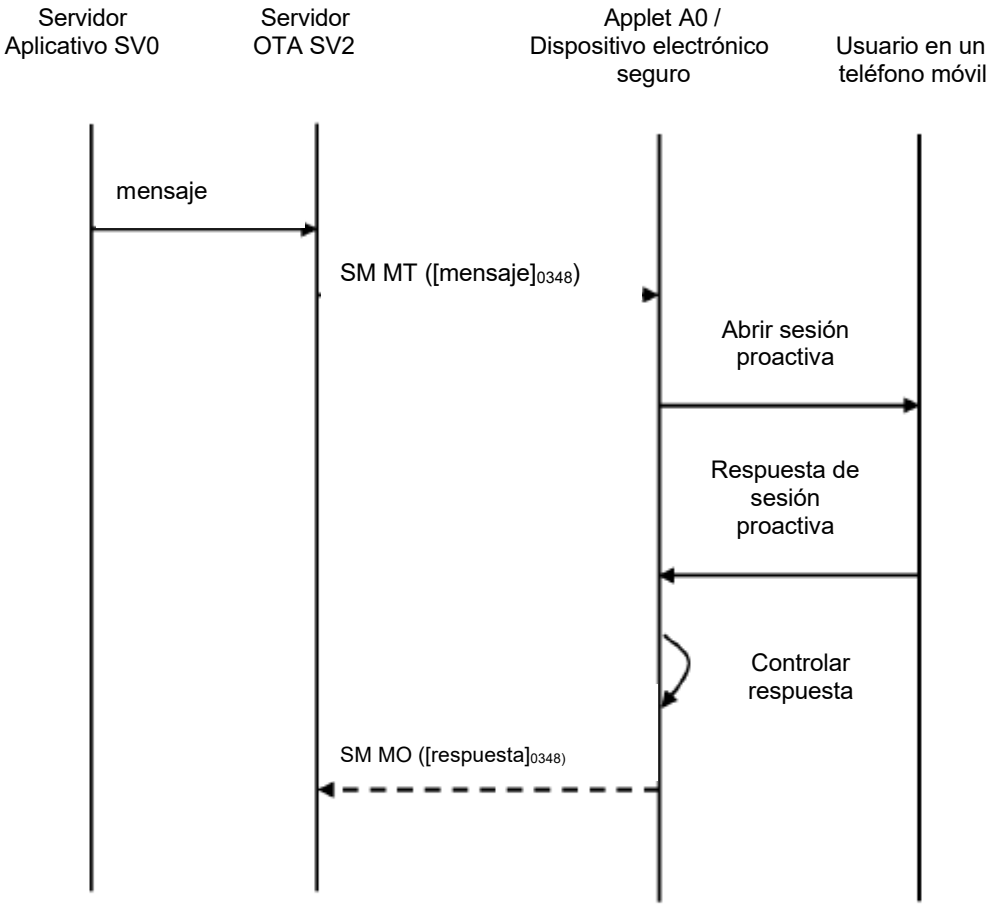

FIG. 2
(Arte anterior)

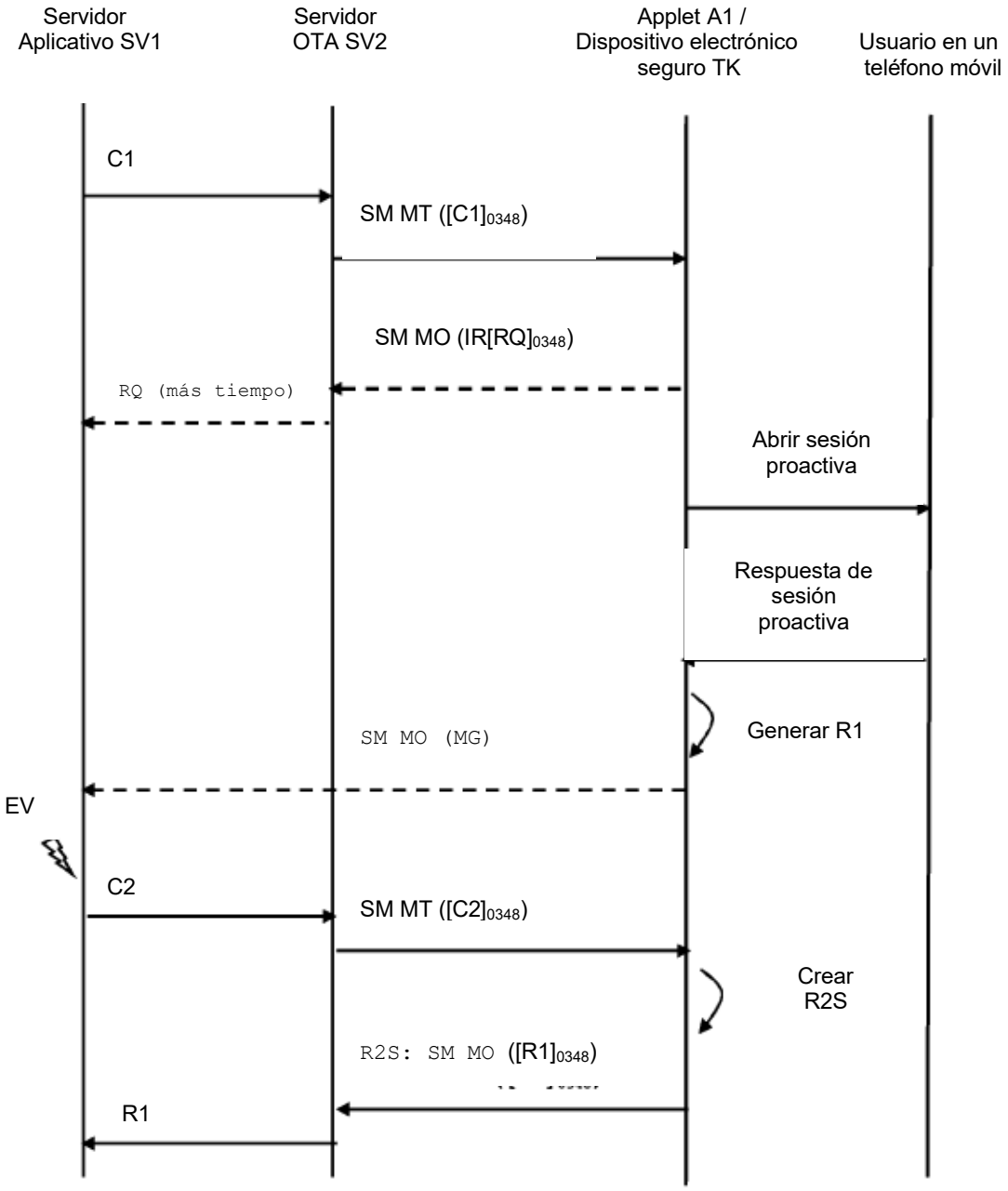
Servidor Aplicativo SV1
Servidor OTA SV2
Applet A1 / Dispositivo electrónico seguro TK
Usuario en un teléfono móvil
C1
SM MT ([C1]0348)
SM MO (IR[RQ]0348)
RQ (más tiempo)
Abrir sesión proactiva
Respuesta de sesión proactiva
Generar R1
SM MO (MG)
EV
C2
SM MT ([C2]0348)
Crear R2S
R2S: SM MO ([R1]0348)
R1

FIG. 3