(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 967 013**

(51) Int. Cl.:

H04W 8/20 (2009.01)
H04L 9/40 (2012.01)
H04W 8/18 (2009.01)
H04W 12/069 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.05.2021 E 21174445 (3)**

(97) Fecha y número de publicación de la concesión europea: **06.09.2023 EP 3917184**

(54) Título: **Procedimiento y dispositivos de gestión de perfiles de comunicación**

(30) Prioridad:

28.05.2020 FR 2005657

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.04.2024

(73) Titular/es:

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

(72) Inventor/es:

KARPINSKI, PAWEL;
MACUDA, JACEK y
WOZNIAK, TOMASZ

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento y dispositivos de gestión de perfiles de comunicación

Técnica anterior

La presente invención se enmarca en el campo de la gestión de perfiles de telecomunicaciones.

De manera conocida, los perfiles de telecomunicaciones utilizados por un terminal son proporcionados por un operador y memorizados en un elemento seguro (tarjeta SIM, entidad eSIM, eUICC) de este terminal.

El estándar GSMA (GSM Association) define una entidad LPA (Local Profile Administration) para la gestión de estos perfiles. Esta entidad LPA realiza la interfaz entre el elemento seguro (eUICC, por ejemplo) y la entidad del operador de gestión de perfiles (por ejemplo, el servidor de gestión de suscripciones SM-DP+ "Subscription Manager Data Preparation+").

De acuerdo con las disposiciones del GSMA, esta entidad LPA se ubica en el sistema operativo o en el elemento seguro del terminal. Esta doble posibilidad de localización de la entidad LPA puede acarrear problemas vinculados a la gestión, la utilización y la actualización de dicha entidad LPA, así como problemas vinculados a la gestión de perfiles.

Esta entidad LPA ofrece una interfaz que permite al usuario del terminal gestionar un perfil memorizado en un elemento seguro de su terminal, por ejemplo para instalar un nuevo perfil en el elemento seguro o para activar, desactivar o eliminar dicho perfil.

Hoy en día es frecuente instalar terminales de comunicación en los coches, por ejemplo, para ofrecer servicios de entretenimiento. Para los fabricantes de estos coches, puede no ser deseable dejar en manos del usuario la gestión de los perfiles de telecomunicaciones para acceder a dichos servicios. A los fabricantes de automóviles les preocupa, en particular, que se les solicite asegurar un servicio posventa en caso de problemas relacionados con la calidad del servicio proporcionado por un operador elegido por el usuario del vehículo. El documento EP 3 029 968, 8 de junio de 2016 (2016-06-08), propone un servidor para el aprovisionamiento de un perfil de abonado a una red de comunicación móvil que comprende un registro del perfil, medios de procesamiento para iniciar el aprovisionamiento del perfil a un terminal de abonado y para crear una solicitud de aprovisionamiento y una solicitud de activación para dicho perfil así como un medio de envío de la solicitud de aprovisionamiento y de la solicitud de activación al terminal.

Por tanto, los mecanismos de gestión de perfiles de comunicación conocidos hasta el momento no están adaptados a estos nuevos servicios.

Exposición de la invención

La invención tiene como objetivo un nuevo mecanismo de gestión de perfiles de comunicación.

Así, según un primer aspecto, la invención se refiere a un dispositivo centralizado de gestión de perfiles de comunicación, incluyendo este dispositivo:

- un módulo de gestión de perfiles capaz de crear dinámicamente una tarea de ejecución para responder a una necesidad de gestión remota de un perfil de comunicación en un elemento seguro integrado en un terminal;

siendo capaz dicho módulo de gestión de perfiles de ejecutar dicha tarea de ejecución

- un módulo de comunicación capaz de establecer en una red un primer canal de comunicación entre esta tarea de ejecución y un gestor de perfiles de comunicación;
- siendo capaz esta tarea de ejecución de obtener dicho perfil de comunicación del gestor a través del primer canal de comunicación;
- siendo capaz este módulo de comunicación de establecer una sesión de comunicación entre esta tarea de ejecución y un agente de comunicación configurado para enviar al elemento seguro, al menos un comando de gestión de este perfil encapsulado en al menos un mensaje enviado por esta tarea de ejecución en el marco de esta sesión; y
- un módulo configurado para eliminar dicha tarea de ejecución cuando se haya llevado a cabo una acción que responda a dicha necesidad.

Correlativamente, la invención se refiere a un procedimiento de gestión de perfiles de comunicación implementado por un dispositivo centralizado de gestión de perfiles de comunicación, incluyendo este procedimiento

- una etapa de creación dinámica de una tarea de ejecución (CLPAi) para responder a una necesidad de gestión remota de un perfil de comunicación en un elemento seguro integrado en un terminal;
- una etapa de ejecución de dicha tarea de ejecución;
- una etapa de establecimiento, en una red, de un primer canal de comunicación entre esta tarea de ejecución y un gestor de perfil de comunicación;

- siendo capaz esta tarea de ejecución de obtener dicho perfil de comunicación del gestor a través del primer canal de comunicación;
- una etapa de establecimiento de una sesión de comunicación entre esta tarea de ejecución y un agente de comunicación configurado para enviar al elemento seguro, al menos un comando de gestión de este perfil encapsulado en al menos un mensaje enviado por esta tarea de ejecución en el marco de esta sesión; y
- una etapa de eliminación de esta tarea de ejecución cuando se haya llevado a cabo una acción que responda a dicha necesidad.

Según un segundo aspecto, la invención se refiere a un agente de comunicación que incluye:

- un primer módulo de comunicación configurado para establecer una sesión de comunicación con una tarea de ejecución de un dispositivo centralizado de gestión de perfiles de comunicación tal como se mencionó anteriormente; y
- un segundo módulo de comunicación configurado para enviar a un elemento seguro integrado en un terminal, al menos un comando para gestionar un perfil encapsulado en al menos un mensaje recibido de esta tarea de ejecución en el marco de esta sesión.

Correlativamente, la invención se refiere a un procedimiento de comunicación implementado por un agente de comunicación, incluyendo este procedimiento:

- una etapa de establecimiento de una sesión de comunicación con una tarea de ejecución de un dispositivo centralizado de gestión de perfiles de comunicación como se mencionó anteriormente;
- una etapa de envío a un elemento seguro integrado en un terminal, de al menos un comando de gestión de un perfil encapsulado en al menos un mensaje recibido de dicha tarea de ejecución en el marco de la sesión.

Así, y de forma general, la invención propone trasladar las funciones de gestión de perfiles de comunicación a un dispositivo centralizado en la red de comunicación, siendo capaz este dispositivo de comunicarse con un agente de comunicación configurado para garantizar la interfaz entre este dispositivo y el elemento seguro.

Visto de otro modo, se puede considerar que la invención propone trasladar las funciones del LPA en la red, desempeñando el agente de comunicación un papel minimalista de puerta de enlace entre este dispositivo y el elemento seguro.

Cuando los terminales están integrados en un automóvil, el fabricante del automóvil puede administrar fácilmente los perfiles de comunicación almacenados en los elementos seguros de estos terminales interconectando su sistema de información con el dispositivo centralizado de gestión de perfiles según la invención.

En el sentido de la invención, y como es sabido, se crea dinámicamente una tarea de ejecución para responder a cualquier necesidad de gestión de un perfil del elemento seguro eUICC (administración, auditoría, instalación, activación, desactivación, eliminación de perfiles) y eliminación cuando se haya llevado a cabo la acción que responde a esta necesidad. Una tarea de ejecución se puede implementar, por ejemplo, en forma de proceso.

De acuerdo con la invención, el agente de comunicación según la invención ofrece al elemento seguro las mismas API (Application Programming Interfaces) definidas por el estándar GSMA; cuando el elemento seguro desea utilizar una función del LPA llama al estándar API, enviando este último una instrucción al dispositivo centralizado en la red para que ejecute la función LPA correspondiente trasladada en la red.

El agente de comunicación puede verse como un proxy. Puede estar integrado o no en el terminal que incluye el elemento seguro. En un ejemplo particular de integración, el proxy (agente de comunicación) puede integrarse en el elemento seguro, del tipo, por ejemplo, eUICC.

La invención también se refiere a un terminal que incluye un agente de comunicación como se mencionó anteriormente y un elemento seguro.

En un modo de realización de la invención, el elemento seguro es del tipo eSIM como se define por el GSMA o del tipo eUICC (embedded UICC).

En un modo de realización de la invención, los comandos son comandos APDU (Application Protocol Data Unit) definidos por el estándar ISO 7816.

Según un modo de realización particular, la tarea de ejecución está configurada para implementar o al menos participar en un mecanismo de autenticación mutua entre el gestor de perfiles y el elemento seguro. Por ejemplo, la tarea de ejecución puede iniciar este mecanismo de autenticación.

Según un modo de realización particular del dispositivo centralizado de gestión de perfiles según la invención, los comandos son, por ejemplo, comandos para cargar un perfil en el elemento seguro y/o para activar o desactivar o eliminar un perfil en el elemento seguro.

En un modo de realización particular, el dispositivo de gestión de perfiles según la invención se caracteriza por que dicha tarea de ejecución está configurada para comunicarse según un protocolo seguro con dicho gestor de perfiles a través del primer canal de comunicación, se establece utilizando un certificado $CERT_{SM}$ compartido entre el gestor de perfiles y el elemento seguro. En este modo de realización particular, los comandos de gestión de perfil están previamente asegurados dentro del gestor de perfiles, mediante la utilización de este certificado compartido antes de enviarlos a través del canal de comunicación seguro establecido entre el gestor de perfiles y la tarea de ejecución. Según un modo de realización particular, la tarea de ejecución CLPAi está además configurada para transmitir los comandos de gestión de perfil al agente de comunicación DAG según un protocolo seguro en el marco de la sesión SC1, utilizando este protocolo seguro un certificado $CERT_{SIM}$ memorizado en el elemento seguro eUICC. El hecho de memorizar el certificado en el elemento seguro refuerza considerablemente la seguridad del procedimiento de gestión de perfiles. Así, en este modo de realización, antes de transmitir un comando de gestión de perfiles al agente de comunicación, el dispositivo centralizado abre el mensaje previamente recibido del gestor de perfiles y encapsulado con el certificado $CERT_{SM}$ del gestor de perfiles y lo encapsula utilizando el certificado $CERT_{SIM}$ utilizado para la sesión de comunicación SC1.

La invención permite así dos tipos de cifrado: un primer tipo de encapsulación de los comandos correspondientes al primer canal de comunicación seguro establecido entre el gestor de perfiles y la tarea de ejecución CLPAi y un segundo tipo de encapsulación de los comandos correspondientes al protocolo seguro de la sesión de comunicación SC1. Por tipo de encapsulación nos referimos a la utilización de un certificado (por ejemplo $CERT_{SIM}$, $CERT_{SM}$) dedicado al aseguramiento de una comunicación (mensajes) entre una primera entidad y una segunda entidad. La seguridad se encuentra así reforzada.

En otro modo de realización particular, cada uno de los tipos de cifrado utiliza un certificado idéntico.

En este modo de realización, el agente de comunicación, por ejemplo su primer módulo de comunicación, está configurado para obtener un certificado memorizado en el elemento seguro y/o para utilizar este certificado para comunicarse según el protocolo seguro con el dispositivo centralizado de gestión de perfiles en el marco de la sesión.

La invención necesita establecer una sesión entre la tarea de ejecución del dispositivo centralizado de gestión de perfiles y el agente de comunicación asociado al elemento seguro. La invención propone en particular dos variantes para establecer esta sesión.

En una primera variante, que se puede calificar de modo “push”, la sesión se establece por iniciativa del dispositivo centralizado de gestión de perfil. Cuando el dispositivo centralizado de gestión de perfiles tiene comandos que enviar al elemento seguro, envía un mensaje de invitación al agente de comunicación para que éste establezca una sesión con el dispositivo centralizado de gestión de perfiles.

Así, según un modo de realización particular de esta primera variante, el dispositivo de gestión de perfil según la invención incluye un módulo de establecimiento de sesión configurado para enviar un mensaje de invitación destinado al agente de comunicación para invitar a este agente a comunicarse a establecer una sesión con el dispositivo centralizado de gestión.

Este mensaje de invitación es un mensaje, preferiblemente firmado y/o cifrado, del tipo, por ejemplo, SMS.

En una segunda variante, que puede calificarse de modo "pull", el agente de comunicación tiene la posibilidad de interrogar, por ejemplo periódicamente, al dispositivo centralizado de gestión de perfiles, iniciando directamente el establecimiento de una sesión hacia este último, sin necesidad de recepción previa, por parte del agente de comunicación, de un mensaje de invitación para iniciar el establecimiento de esta sesión. En el marco de esta sesión una vez establecida, y a iniciativa del agente de comunicación, el dispositivo centralizado de gestión de perfiles puede enviar comandos al elemento seguro siempre que dichos comandos estén disponibles y destinados al elemento seguro.

Según un modo particular de esta segunda variante de realización, el dispositivo centralizado de gestión de perfiles según la invención incluye un módulo de establecimiento de sesión configurado para recibir solicitudes de interrogación procedentes del agente de comunicación, estando configurado el módulo de establecimiento de sesión para establecer una sesión con el agente de comunicación en respuesta a dicha solicitud.

Según un modo de realización particular, el dispositivo centralizado de gestión de perfiles incluye un módulo de interfaz capaz de recibir una solicitud de administración de un tercero, por ejemplo para:

- cargar el perfil de comunicación en el elemento seguro; o
- para activar, desactivar o eliminar el perfil de comunicación en el elemento seguro.

Esta solicitud de administración puede ser enviada por el propietario del terminal, por el usuario del terminal o por una entidad de gestión del terminal, por ejemplo por una entidad de gestión de una flota de terminales a la que pertenece este terminal.

En un modo de realización particular, los procedimientos se implementan mediante programas informáticos.

Por consiguiente, la invención se refiere también a un programa informático sobre un soporte de grabación, siendo susceptible este programa de implementarse en un dispositivo o, más generalmente, en un ordenador. Este programa incluye instrucciones adaptadas a la implementación de un procedimiento de gestión de perfiles como se describe anteriormente.

Cada uno de estos programas puede utilizar cualquier lenguaje de programación y estar en forma de código fuente, código objeto o código intermedio entre el código fuente y el código objeto, tal como en una forma parcialmente compilada o en cualquier otra forma deseable.

La invención también se refiere a un soporte de información o un soporte de grabación legibles por un ordenador, y que incluye instrucciones de un programa informático como se mencionó anteriormente.

Los soportes de información o de grabación pueden ser cualquier entidad o dispositivo capaz de almacenar programas. Por ejemplo, los soportes pueden incluir un medio de almacenamiento, tal como una ROM, por ejemplo un CD ROM o un circuito microelectrónico ROM, o también un medio de grabación magnético, por ejemplo un disquete (floppy disc) o un disco duro, o una memoria flash.

Por otro lado, los soportes de información o de grabación pueden ser soportes transmisibles tales como una señal eléctrica u óptica, que puede transmitirse a través de un cable eléctrico u óptico, por radioenlace, por enlace óptico inalámbrico o por otros medios.

Los programas según la invención pueden cargarse en particular en una red de tipo Internet.

Alternativamente, cada soporte de información o de grabación puede ser un circuito integrado en el que se incorpora un programa, estando adaptado el circuito para ejecutar o para utilizarse en la ejecución de uno de los procedimientos según la invención.

Breve descripción de los dibujos

Otras características y ventajas de la presente invención se desprenderán de la descripción que se hace a continuación, con referencia a los dibujos adjuntos que ilustran un ejemplo de realización sin carácter limitativo. En las figuras:

[Fig. 1] la figura 1 representa un dispositivo centralizado de gestión de perfiles y un agente de comunicación conforme a un modo de realización particular en su entorno;

[Fig. 2] la figura 2 representa las etapas principales de un procedimiento de gestión de perfiles y un procedimiento de comunicación de acuerdo con la invención para descargar un perfil de comunicación en un elemento seguro; y

[Fig. 3] la figura 3 representa las etapas principales de un procedimiento de gestión de perfiles y un procedimiento de comunicación de acuerdo con la invención para activar un perfil de comunicación en un elemento seguro.

Descripción de los modos de realización

La figura 1 representa, en su entorno, un terminal T y un dispositivo centralizado CLPA de gestión de perfiles de comunicación de acuerdo con modos de realización particulares de la invención.

En el modo de realización descrito aquí, el terminal T está integrado en un automóvil no representado. En este ejemplo, el terminal T está gestionado remotamente por el sistema de información SI-AUTO del fabricante de este automóvil.

Este terminal T incluye un agente de comunicación DAG de acuerdo con la invención y un elemento seguro eUICC.

El elemento seguro eUICC incluye un identificador único eid y un certificado criptográfico $CERT_{SIM}$. El elemento seguro puede memorizar uno o más perfiles de comunicación.

En la figura 1 también se representa un gestor de perfiles de comunicación SM-DP+. Este gestor de perfiles SM-DP+ memoriza varios perfiles, incluido un perfil $PROF_{eid}$ destinado al elemento seguro eUICC del terminal T. El gestor de perfiles también garantiza una función de seguridad de perfiles y una función de asignación respectiva del perfil a la eUICC a la que está destinado.

El terminal T, el dispositivo centralizado CLPA de gestión de perfiles, el sistema de información SI-AUTO del fabricante de automóviles y el gestor de perfiles de comunicación SM-DP+ se comunican a través de una red NET. Cada uno incluye para ello un módulo de comunicación COM-NET.

Esta red NET es por ejemplo la red de Internet o una red de telefonía móvil de tipo 2G, 3G, 4G o 5G.

En el modo de realización descrito aquí, el dispositivo centralizado CLPA de gestión de perfiles incluye un módulo de gestión de perfiles MGP, incluyendo este módulo:

- un submódulo de interfaz IF capaz de recibir solicitudes de administración RAQ, por ejemplo del propietario del terminal T o del sistema de informaciones SI-AUTO del fabricante de automóviles;
- un submódulo MI de gestión de tareas de ejecución capaz de crear, ejecutar y eliminar una tarea de ejecución CLPAi para gestionar los perfiles de comunicación del elemento seguro eUICC desde la red NET; y
- un submódulo MES de establecimiento de sesión, capaz de establecer y terminar una sesión de comunicación SC1 entre una tarea de ejecución CLPAi y el agente de comunicación DAG. En el modo de realización descrito aquí, estas sesiones de comunicación SC1 cumplen con el protocolo TLS y utilizan el certificado $CERT_{SIM}$ del elemento seguro eUICC.

El certificado $CERT_{SIM}$ permite asegurar los intercambios de la sesión SC1 entre el agente de comunicación DAG y el dispositivo centralizado CLPA de gestión de perfiles.

En el modo de realización descrito aquí, el dispositivo centralizado CLPA de gestión de perfiles es capaz de establecer un canal de comunicación CC2 entre una tarea de ejecución CLPAi y el gestor de perfiles SM-DP+.

En el modo de realización descrito aquí, este canal de comunicación CC2 es seguro e implementa el protocolo TLS; utiliza un certificado $CERT_{SM}$ del gestor de perfiles SM-DP+ para asegurar los intercambios entre el dispositivo centralizado CLPA y el gestor de perfiles SM-DP+.

El protocolo TLS puede sustituirse por otro protocolo criptográfico.

Certificados distintos de los utilizados para asegurar el canal de comunicación CC2 y la sesión de comunicación SC1 también se pueden utilizar para asegurar los intercambios entre el gestor de perfiles de comunicación SM-DP+ y el elemento seguro eUICC del terminal T.

Como se describe más adelante, la tarea de ejecución CLPAi puede utilizar el canal de comunicación seguro CC2 para descargar un perfil de comunicación PROF desde el gestor de perfiles SM-DP+, por ejemplo el perfil $PROF_{eid}$ destinado al elemento seguro eUICC del terminal T.

Los mensajes enviados por la tarea de ejecución CLPAi al agente de comunicación DAG encapsulan comandos de gestión de perfiles destinados al elemento seguro eUICC. En el ejemplo de realización descrito aquí, estos comandos son comandos APDU.

Estos comandos pueden ser en particular:

- un comando APDU para instalar un perfil en el elemento seguro eUICC, por ejemplo el perfil $PROF_{eid}$;
- un comando APDU para activar, desactivar o eliminar un perfil instalado en el elemento seguro eUICC.

El agente de comunicación DAG incluye un módulo COM-SIM configurado para enviar al elemento seguro eUICC los comandos de gestión de perfil (por ejemplo comandos APDU) encapsulados en los mensajes recibidos desde el dispositivo centralizado CLPA de gestión de perfiles de comunicación.

Los comandos de gestión de perfiles se aseguran inicialmente dentro del gestor de perfiles SM-DP+, mediante la utilización de un certificado $CERT_3$ compartido entre el elemento seguro eUICC y el gestor de perfiles SM-DP+, antes de su envío, a través del canal de comunicación seguro CC2. Se asegura así un doble cifrado que permite aumentar la seguridad de los comandos.

La transmisión de los comandos de gestión de perfil entre el dispositivo centralizado CLPA y el agente de comunicación DAG es segura (encapsulación de los comandos en los mensajes) mediante la utilización del certificado $CERT_{SIM}$ del elemento seguro eUICC. Como ya se mencionó anteriormente, habiendo sido inicialmente protegidos los comandos dentro del gestor de perfiles SM-DP+, mediante la utilización de un certificado $CERT_3$, aseguramos, nuevamente, en el marco de la sesión SC1, esta vez, un doble cifrado de comandos.

El canal de comunicación CC2 permite una encapsulación segura de los comandos de gestión transmitidos entre el gestor de perfiles SM-DP+ y el dispositivo centralizado CLPA, utilizando el certificado $CERT_{SM}$ del gestor de perfiles SM-DP+.

Así, antes de transmitir un comando de gestión de perfiles al agente de comunicación DAG, el dispositivo centralizado CLPA abre el mensaje previamente recibido del gestor de perfiles SM-DP+ y encapsulado con el certificado $CERT_{SM}$, y lo encapsula utilizando el certificado $CERT_{SIM}$ utilizado durante la sesión de comunicación SC1, garantizando así la seguridad de la transmisión entre el dispositivo centralizado CLPA y el agente de comunicación DAG.

En el modo de realización descrito aquí, una tarea de ejecución CLPAi del dispositivo centralizado CLPA está configurada para implementar o participar en un mecanismo de autenticación mutua entre dicho gestor de perfiles y el elemento seguro.

El submódulo MES de establecimiento de sesión del dispositivo centralizado CLPA es capaz de establecer y terminar una sesión de comunicación SC1 entre una tarea de ejecución CLPAi y el agente de comunicación DAG.

En el modo de realización descrito aquí, este submódulo MES puede funcionar en modo "pull" y en modo "push".

En el modo "push", este submódulo de establecimiento de sesión MES envía un mensaje de invitación destinado al agente de comunicación DAG para invitar a este agente de comunicación a establecer una sesión de comunicación SC1 con el dispositivo centralizado CLPA de gestión.

Más precisamente, en un modo de realización particular, el sistema de informaciones SI-AUTO envía una solicitud de administración al dispositivo centralizado CLPA de gestión de perfiles. Después de la recepción de la solicitud por parte del dispositivo centralizado CLPA, el submódulo MES de establecimiento de sesión envía un mensaje MINV al agente de comunicación DAG asociado al elemento seguro eUICC para invitarle a establecer una sesión de comunicación SC1 con el sistema centralizado CLPA.

En una variante de realización del modo PUSH, se envía una solicitud de administración desde el terminal al sistema de información SI-AUTO. El sistema de información recibe esta solicitud y la envía entonces al dispositivo centralizado CLPA de gestión de perfiles como se describió anteriormente.

En otro modo de realización particular, el submódulo de establecimiento de sesión MES envía directamente este mensaje de invitación MINV al agente de comunicación DAG, por ejemplo en forma de un SMS firmado y/o cifrado verificable por el agente DAG.

En el modo "pull", el submódulo de establecimiento de sesión MES está configurado para recibir solicitudes de interrogación del agente de comunicación DAG y para establecer una sesión SC1 con el agente de comunicación en respuesta a dicha solicitud cuando el dispositivo centralizado CLPA de gestión de perfiles tiene al menos un comando de gestión de perfil para enviar al elemento seguro eUICC.

En el modo de realización descrito aquí, el submódulo de interfaz IF del dispositivo centralizado CLPA de gestión de perfiles está configurado para recibir solicitudes de administración RAQ, por ejemplo del propietario del terminal T o del sistema de informaciones SI-AUTO del fabricante de automóviles.

En la práctica, este submódulo de interfaz IF puede comunicarse con una aplicación de software del terminal T o del sistema de informaciones SI-AUTO. Esta aplicación de software puede denominarse agente externo AE. Permite presentar al usuario los perfiles del gestor SM-DP+ que se pueden descargar en un elemento seguro eUICC determinado. También ofrece un menú que permita al usuario activar, desactivar o eliminar un perfil instalado en un elemento seguro.

Con referencia a la figura 2, describiremos ahora las etapas principales de un procedimiento de gestión de perfiles y las etapas principales de un procedimiento de comunicación de acuerdo con un modo de realización particular de la invención para instalar un perfil en un elemento seguro.

Más precisamente, asumimos que un usuario desea descargar un nuevo perfil $PROF_{eid}$ en el elemento seguro eUICC de su terminal T; para ello, escanea (etapa T10) un código QR proporcionado por el operador de telecomunicaciones.

Esta acción desencadena el envío de una solicitud RACT_DWLD de descarga de perfiles al sistema de informaciones SI-AUTO del fabricante del automóvil, incluyendo esta solicitud el identificador eid de este elemento seguro, el identificador $PROF_{eid}$ de este perfil y un código de activación CA, permitiendo este código de activación CA al sistema de información SI_AUTO verificar la validez de la solicitud.

Al recibir esta solicitud, el agente externo AE del sistema de informaciones SI-AUTO envía (etapa S20) una solicitud de administración RADM_DWLD al módulo MPG de gestión de perfiles del dispositivo centralizado CLPA de gestión de perfiles. En el ejemplo descrito aquí, esta solicitud es la solicitud downloadProfile(eid) definida en el documento "Especificación Técnica GSMA SGP.22 RSP Versión 2.2", en adelante [1].

El submódulo MI de gestión de tareas de ejecución crea entonces (etapa M30) una tarea de ejecución CLPAi para descargar el perfil $PROF_{eid}$ desde el gestor SM-DP+ al elemento seguro eUICC.

El submódulo MES de establecimiento de sesión envía (etapa M40) un SMS MINV firmado y/o cifrado al agente de comunicación DAG asociado con el elemento seguro eUICC para invitarlo a establecer una sesión de comunicación SC1 con la tarea de ejecución CLPAi.

Se establece una sesión de comunicación segura TLS SC1 (etapa D50) entre el agente de comunicación DAG y la tarea de ejecución CLPAi, utilizando esta sesión el certificado $CERT_{SIM}$ del elemento seguro eUICC.

Durante una etapa C60, la tarea de ejecución CLPAi interroga al elemento seguro eUICC para obtener las informaciones que se proporcionará al gestor de perfiles SM-DP+. En el modo de realización descrito aquí, la tarea de ejecución CLPAi utiliza la función GetEUICCInfo de [1].

Durante una etapa C70, la tarea de ejecución CLPAi crea un canal de comunicación TLS CC2 con el gestor de perfiles SM-DP+ utilizando el certificado $CERT_{SM}$ de este gestor.

Durante una etapa C80, la tarea de ejecución CLPAi implementa un mecanismo de autenticación mutua entre el elemento de seguridad eUICC y el gestor de perfiles SM-DP+. En el modo de realización descrito aquí, esta etapa utiliza las funciones ES10b. GetEUICCChallenge, ES9+.InitiateAutentication, ES10b.AuthenticateServer y ES9+.AutenticateClient de [1].

En un modo de realización particular, no representado aquí, la función ES10b.GetEUICCChallenge se realiza entre la etapa C60 y la etapa C70 y no durante la etapa C80.

La tarea de ejecución CLPAi descarga (etapa C90) el perfil del gestor de perfiles SP-DP+ a través del canal de comunicación TLS CC2. En el modo de realización descrito aquí, se utiliza la función ES9+.GetBoundProfilePackage de [1] para ello.

La tarea de ejecución CLPAi envía (etapa C100) al agente de comunicación DAG, a través de la sesión TLS SC1, mensajes asegurados por el certificado $CERT_{SIM}$, encapsulando estos mensajes comandos APDU para instalar el perfil en el elemento seguro eUICC. Estos comandos APDU se transmiten a través del módulo COM-SIM al elemento seguro eUICC. En el modo de realización descrito aquí, la tarea de ejecución CLPAi utiliza la función LoadBoundProfilePackage de [1] para transferir el perfil al elemento seguro eUICC.

Si la descarga se realiza correctamente, la tarea de ejecución de CLPAi envía un mensaje de instalación exitosa de ES9+.HandleNotification al gestor de perfiles SM-DP+ (etapa C110) y un mensaje de notificación ES10BRemoveNotificationfromList al elemento seguro eUICC (etapa C120).

Durante una etapa C130, la tarea de ejecución CLPAi finaliza la sesión de comunicación SC1.

Durante una etapa C140, la tarea de ejecución finaliza el canal de comunicación CC2 con el gestor de perfil de comunicación SM-DP+.

Durante una etapa M140, el submódulo MES del módulo de gestión de perfiles envía al agente externo AE del sistema de información SI-AUTO información según la cual el perfil solicitado ha sido descargado en el elemento seguro eUICC.

El submódulo MI de gestión de tareas de ejecución finaliza/elimina (etapa M50) la tarea de ejecución CLPAi.

La figura 3 representa las principales etapas de un procedimiento de gestión de perfiles y las principales etapas de un procedimiento de comunicación de acuerdo con un modo de realización particular de la invención para activar un perfil en un elemento seguro.

Más precisamente, se supone que el fabricante del automóvil desea activar el perfil $PROF_{eid}$ en el elemento seguro eUICC del terminal T.

Para ello, utiliza el agente externo AE del sistema de informaciones SI-AUTO para enviar (etapa S200) una solicitud de administración RADM_ACT para la activación del perfil (eid, $PROF_{eid}$) al módulo MGP (más precisamente al submódulo de interfaz IF) de gestión de perfiles del dispositivo centralizado CLPA de gestión de perfiles. En el ejemplo descrito aquí, esta solicitud es la solicitud enableProfile(eid) de [1].

El submódulo MI de gestión de tareas de ejecución crea entonces (etapa M300) una tarea de ejecución CLPAi para activar el perfil $PROF_{eid}$ en el elemento seguro eUICC.

El submódulo MES de establecimiento de sesión envía (etapa M400) un SMS firmado MINV al agente de comunicación DAG asociado con el elemento seguro eUICC para invitarle a establecer una sesión de comunicación SC1 con la tarea de ejecución CLPAi.

Se establece una sesión de comunicación segura TLS SC1 (etapa D500) entre el agente de comunicación DAG y la tarea de ejecución CLPAi, utilizando esta sesión el certificado $CERT_{SIM}$ del elemento seguro eUICC.

La tarea de ejecución CLPAi envía (etapa C1000) al agente de comunicación DAG, a través de la sesión TLS SC1, mensajes asegurados por el certificado $CERT_{SIM}$, encapsulando estos mensajes comandos APDU para activar el perfil en el elemento seguro eUICC. Estos comandos APDU se transmiten a través del módulo COM-SIM al elemento seguro eUICC. En el modo de realización descrito aquí, la tarea de ejecución CLPAi utiliza la función ES10cEnable de [1] para activar el perfil $PROF_{eid}$ en el elemento seguro eUICC.

Si la activación se realiza correctamente, la tarea de ejecución CLPAi finaliza la sesión de comunicación SC1 (etapa C1300).

El submódulo MI de gestión de tareas de ejecución finaliza/elimina (etapa M500) la tarea de ejecución CLPAi.

Durante una etapa M140, el submódulo MES del módulo de gestión de perfiles envía al agente externo AE del sistema de informaciones SI-AUTO información según la cual el perfil $PROF_{eid}$ ha sido activado en el elemento seguro eUICC.

REIVINDICACIONES

1. Dispositivo centralizado (CLPA) de gestión de perfiles de comunicación, incluyendo este dispositivo:

- un módulo de gestión de perfiles (MGP) capaz de crear dinámicamente una tarea de ejecución (CLPAi) para responder a una necesidad de gestión remota de un perfil de comunicación ($PROF_{eid}$) en un elemento seguro (eUICC) integrado en un terminal (T)
- siendo capaz dicho módulo de gestión de perfiles (MGP) de ejecutar dicha tarea de ejecución (CLPAi);
- un módulo de comunicación (COM-NET) capaz de establecer en una red un primer canal de comunicación (CC2) entre dicha tarea de ejecución (CLPAi) y un gestor (SM-DP+) de perfiles de comunicación;
- siendo capaz dicha tarea de ejecución (CLPAi) de obtener dicho perfil de comunicación ($PROF_{eid}$) de dicho gestor (SM-DP+) a través de dicho primer canal de comunicación (CC2);
- siendo capaz dicho módulo de comunicación (COM-NET) de establecer una sesión de comunicación (SC1) entre dicha tarea de ejecución (CLPAi) y un agente de comunicación (DAG) según la reivindicación 10 configurado para enviar a dicho elemento seguro (eUICC), al menos un comando de gestión de dicho perfil ($PROF_{eid}$), estando dicho comando de gestión encapsulado en al menos un mensaje enviado por dicha tarea de ejecución (CLPAi) en el marco de dicha sesión (SC1); y
- un submódulo (MI) configurado para eliminar dicha tarea de ejecución (CLPAi) cuando se ha llevado a cabo una acción que responde a dicha necesidad.

2. Dispositivo centralizado (CLPA) de gestión de perfiles según la reivindicación 1, caracterizado por que dicha tarea de ejecución (CLPAi) está configurada para implementar o al menos participar en un mecanismo de autenticación mutua entre dicho gestor de perfiles (SM-DP+) y dicho elemento seguro (eUICC).

3. Dispositivo centralizado (CLPA) de gestión de perfiles según la reivindicación 1 o 2, caracterizado por que dicho al menos un comando es al menos un comando para cargar dicho perfil en dicho elemento seguro y/o para activar o deshabilitar o eliminar dicho perfil de dicho elemento seguro (eUICC).

4. Dispositivo (CLPA) de gestión de perfiles según una de las reivindicaciones 1 a 3, caracterizado por que dicha tarea de ejecución (CLPAi) está configurada para comunicarse según un protocolo seguro con dicho agente (DAG) en el marco de dicha al menos una sesión (SC1), utilizando dicho protocolo seguro un certificado ($CERT_{SIM}$) memorizado en dicho elemento seguro (eUICC).

5. Dispositivo (CLPA) de gestión de perfiles según una de las reivindicaciones 1 a 3, caracterizado por que dicha tarea de ejecución (CLPAi) está configurada para comunicarse según un protocolo seguro con dicho gestor de perfiles (SM-DP+) en el primer canal de comunicación (CC2), utilizando dicho protocolo seguro un certificado ($CERT_{SM}$) memorizado en dicho gestor de perfil (SM-DP+).

6. Dispositivo (CLPA) de gestión de perfiles según cualquiera de las reivindicaciones 1 a 5, caracterizado por que incluye un módulo de establecimiento de sesión (MES) configurado para enviar un mensaje de invitación (MINV) a dicho agente de comunicación (DAG) para invitar a dicho agente de comunicación a establecer dicha sesión con dicho dispositivo centralizado (CLPA) de gestión.

7. Dispositivo (CLPA) de gestión de perfiles según la reivindicación 6, caracterizado por que dicho mensaje de invitación es un mensaje firmado y/o cifrado de tipo SMS.

8. Dispositivo (CLPA) de gestión de perfiles según cualquiera de las reivindicaciones 1 a 5, caracterizado por que incluye un módulo de establecimiento de sesión (MES) configurado para recibir solicitudes de interrogación de dicho agente de comunicación (DAG), estando configurado dicho módulo (MES) establecer dicha sesión con dicho agente de comunicación en respuesta a dicha solicitud.

9. Dispositivo (CLPA) según la reivindicación 1, caracterizado por que comprende un módulo de interfaz (IF) capaz de recibir una solicitud de administración de un tercero para:

- cargar dicho perfil de comunicación ($PROF_{eid}$) en dicho elemento seguro (eUICC); o
- activar, desactivar o eliminar dicho perfil de comunicación ($PROF_{eid}$) de dicho elemento seguro (eUICC).

10. Agente de comunicación (DAG) que incluye:

- un primer módulo de comunicación (COM-NET) configurado para establecer una sesión de comunicación (SC1) con una tarea de ejecución (CLPAi) de un dispositivo centralizado (CLPA) de gestión de perfiles de comunicación según la reivindicación 1; y
- un segundo módulo de comunicación (COM-SIM) configurado para enviar, a un elemento seguro (eUICC) integrado en un terminal (T), al menos un comando de gestión de un perfil ($PROF_{eid}$), encapsulado en un mensaje recibido de dicha tarea de ejecución (CLPAi) en el marco de dicha sesión.

11. Agente de comunicación (DAG) según la reivindicación 10, caracterizado por que está configurado para obtener un certificado ($CERT_{SIM}$) memorizado en dicho elemento seguro (eUICC) y/o para utilizar este certificado ($CERT_{SIM}$)

para comunicarse según un protocolo seguro con dicho dispositivo centralizado (CLPA) de gestión de perfiles en el marco de dicha sesión.

12. Terminal (T) que incluye un agente de comunicación (DAG) según cualquiera de las reivindicaciones 10 u 11 y un elemento seguro (eUICC).

13. Procedimiento de gestión de perfiles de comunicación implementado por un dispositivo centralizado (CLPA) de gestión de perfiles de comunicación, incluyendo este procedimiento:

- una etapa de creación dinámica de una tarea de ejecución (CLPAi) para responder a una necesidad de gestión de forma remota de un perfil de comunicación ($PROF_{eid}$) en un elemento seguro (eUICC) integrado en un terminal (T);
- una etapa de ejecución de dicha tarea de ejecución (CLPAi);
- una etapa de establecimiento, en una red, un primer canal de comunicación (CC2) entre dicha tarea de ejecución (CLPAi) y un gestor (SM-DP+) de perfiles de comunicación;
- siendo capaz dicha tarea de ejecución (CLPAi) de obtener dicho perfil de comunicación ($PROF_{eid}$) de dicho gestor (SM-DP+) a través de dicho primer canal de comunicación (CC2);
- una etapa de establecimiento de una sesión de comunicación (SC1) entre dicha tarea de ejecución (CLPAi) y un agente de comunicación (DAG) que está configurado para enviar, a dicho elemento seguro (eUICC), al menos un comando de gestión de dicho perfil ($PROF_{eid}$) encapsulado en al menos un mensaje enviado por dicha tarea de ejecución (CLPAi) en el marco de dicha sesión (SC1); y
- una etapa de eliminación de dicha tarea de ejecución (CLPAi) cuando se ha llevado a cabo una acción que responde a dicha necesidad.

14. Procedimiento de comunicación implementado por un agente de comunicación (DAG), incluyendo este procedimiento:

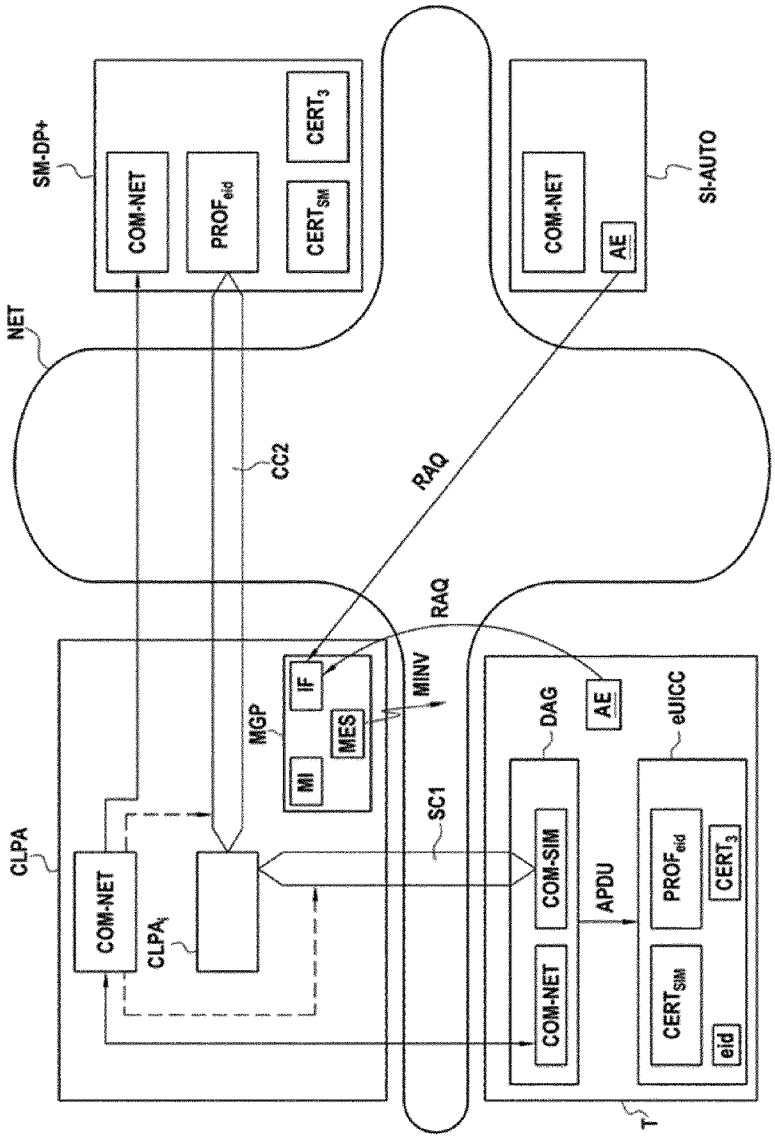
- una etapa de establecimiento de una sesión de comunicación (SC1) con una tarea de ejecución (CLPAi) de un dispositivo centralizado (CLPA) de gestión de perfiles de comunicación según la reivindicación 13;
- una etapa de envío, a un elemento seguro (eUICC) integrado en un terminal (T), de al menos un comando de gestión de un perfil ($PROF_{eid}$) encapsulado en al menos un mensaje recibido de dicha tarea de ejecución (CLPAi) en el marco de dicha sesión.

15. Programa informático que incluye instrucciones para la ejecución de un procedimiento de gestión de perfil según la reivindicación 13, cuando dicho programa se ejecuta mediante un ordenador (CLPA).

16. Programa informático que incluye instrucciones para la ejecución de un procedimiento de comunicación según la reivindicación 14, cuando dicho programa es ejecutado por un ordenador (DAG).

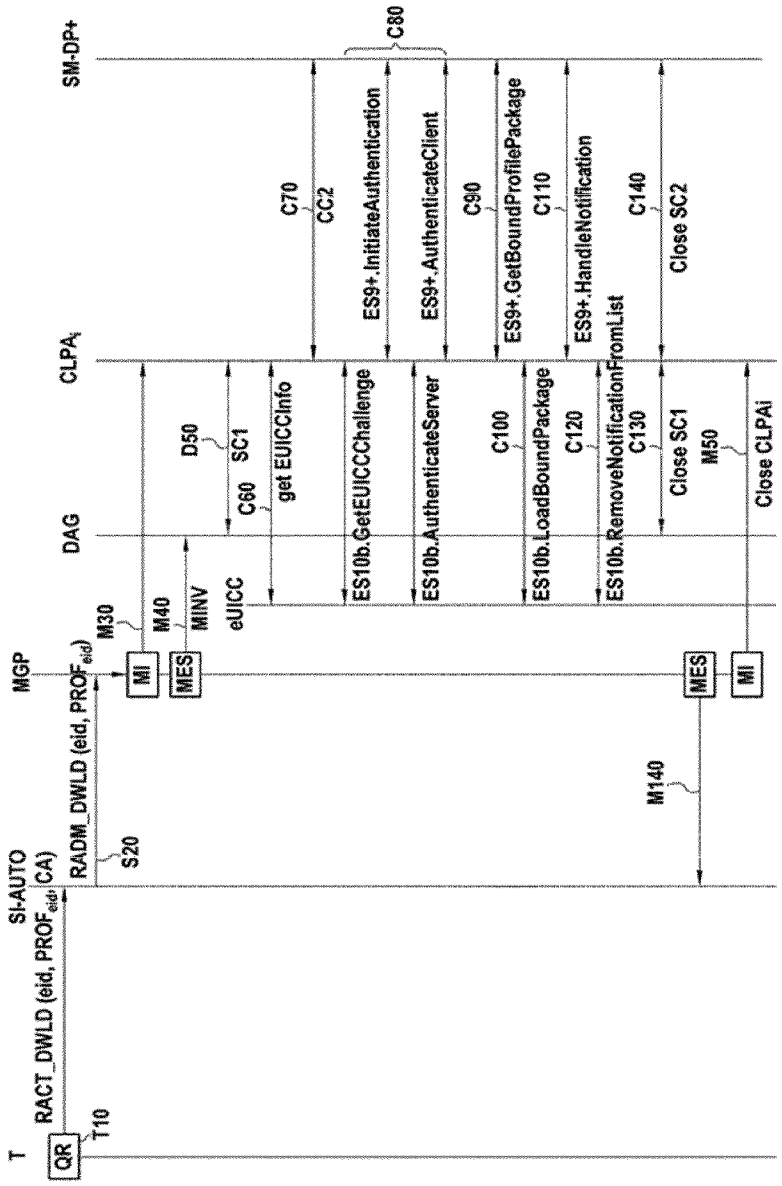
[Fig. 1]

[Fig. 1]


SM-DP+
COM-NET
PROF eid
CERT 3
CERT SM
SI-AUTO
COM-NET
AE
NET
CC2
RAQ
RAQ
MINV
IF
MES
MI
MGP
DAG
AE
eUICC
SC1
CLPA
COM-NET
CLPA i
COM-SIM
APDU
PROF eid
CERT 3
COM-NET
CERT SIM
eid
T

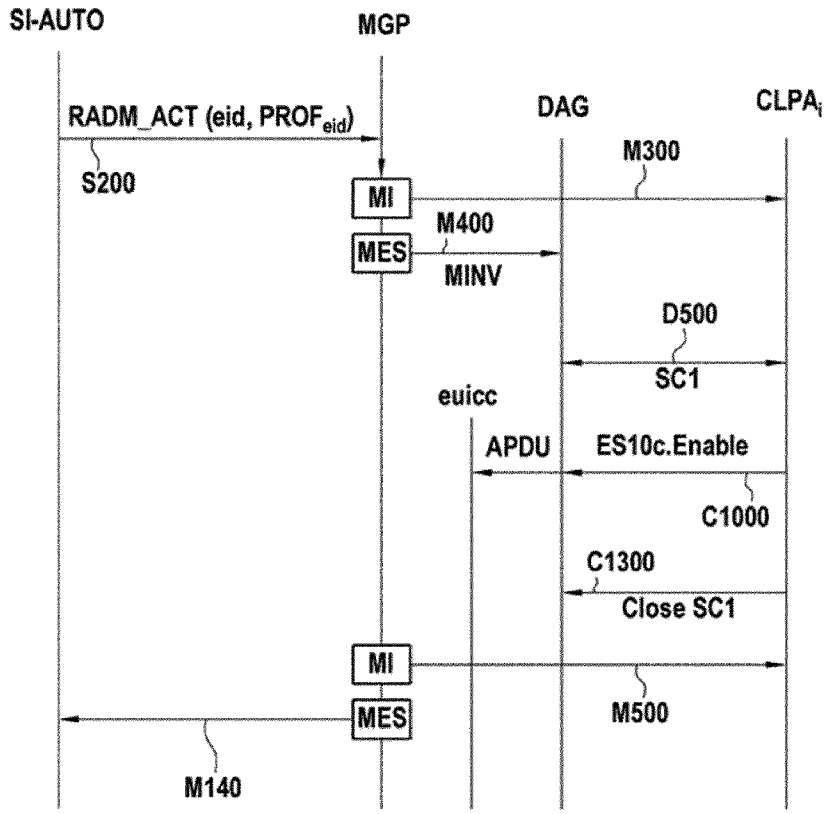
[Fig. 2]

[Fig. 2]


T
SI-AUTO
MGP
DAG
CLPAi
SM-DP+
QR
MI
MES
MES
MI
RACT_DWLD (eid, PROF eidi CA)
RADM_DWLD (eid, PROF eid)
T10
S20
M30
M40
MINV
eUICC
D50
SC1
C60
get EUICCInfo
ES10b.GetEUICCChallenge
ES10b.AuthenticateServer
C100
ES10b.LoadBoundPackage
C120
ES10b.RemoveNotificationFromList
C130
Close SC1
M50
Close CLPAi
M140
C70
CC2
ES9+.InitiateAuthentication
C80
ES9+.AuthenticateClient
C90
ES9+.GetBoundProfilePackage
C110
ES9+.HandleNotification
C140
Close SC2

[Fig. 3]

[Fig. 3]


SI-AUTO
MGP
DAG
CLPA$_i$
RADM_ACT (eid, PROF$_{eid}$)
S200
MI
M300
M400
MES
MINV
D500
SC1
euicc
APDU
ES10c.Enable
C1000
C1300
Close SC1
MI
M500
MES
M140