(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 979 346**

(51) Int. Cl.:

H04L 9/40	(2012.01)	***H04W 52/02***	(2009.01)
G06F 13/16	(2006.01)	***H04W 4/12***	(2009.01)
G06F 13/28	(2006.01)	***H04W 12/02***	(2009.01)
G06F 13/40	(2006.01)	***H04W 12/0431***	(2011.01)
H04L 67/125	(2012.01)	***H04W 88/02***	(2009.01)
H04W 4/14	(2009.01)	***H04W 88/06***	(2009.01)
H04W 4/50	(2008.01)		
H04W 4/70	(2008.01)		
H04W 12/37	(2011.01)		
H04W 80/06	(2009.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.09.2014 E 21154414 (3)**

(97) Fecha y número de publicación de la concesión europea: **21.02.2024 EP 3832982**

(54) Título: **Comunicación segura con un dispositivo móvil**

(30) Prioridad:

13.09.2013 GB 201316370
16.10.2013 GB 201318339
30.05.2014 GB 201409652
30.05.2014 GB 201409641
30.05.2014 GB 201409643
30.05.2014 GB 201409663
22.08.2014 GB 201415003
22.08.2014 GB 201414999
22.08.2014 GB 201414997
09.09.2014 GB 201415927

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.09.2024

(73) Titular/es:

VODAFONE GLOBAL ENTERPRISE LIMITED (50.0%)
Vodafone House The Connection
Newbury Berkshire RG14 2FN, GB y
DABCO LIMITED (50.0%)

(72) Inventor/es:

BOURNE, SOPHIE NICOLE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Comunicación segura con un dispositivo móvil

Campo de la invención

La presente invención se refiere a un procedimiento y sistema para comunicarse de forma segura con un dispositivo móvil y, en particular, un dispositivo de máquina a máquina (M2M).

Antecedentes de la invención

Los dispositivos de máquina a máquina (M2M) suelen ser numerosos, difíciles de alcanzar y tienen capacidades limitadas (debido al bajo coste, el tamaño pequeño, la baja potencia de procesamiento o la duración limitada de la batería). Todo ello hace que su gestión, muchas veces remota, sea muy complicada. Además, los dispositivos M2M a menudo necesitan gestionarse de forma segura. Por ejemplo, pueden contener información que sea comercialmente sensible y/o confidencial para la una o más entidades que gestionan y/o poseen dichos dispositivos. Es necesario gestionarlos y comunicarse con ellos de forma remota y de forma segura, al mismo tiempo que se respetan estas limitaciones.

Un planteamiento es proporcionar a los dispositivos M2M claves PKI que se utilizan para asegurar las comunicaciones con un servidor o gestor de dispositivos. Sin embargo, esto aumenta la complejidad y requiere el mantenimiento de dicho sistema de aprovisionamiento.

Otro planteamiento consiste en utilizar material criptográfico derivado de una clave subyacente. Sin embargo, si esta clave alguna vez se ve comprometida, una escucha clandestina que haya grabado comunicaciones anteriores puede descifrar estos mensajes anteriores. Por lo tanto, se requiere un sistema y un procedimiento que permita que los dispositivos M2M puedan comunicarse de forma más fiable y segura.

Master Thesis et al: "Leveraging Public-key-based Authentication for the Internet of Things", Master Thesis describe el aprovechamiento de la autenticación basada en clave pública para la Internet de las cosas. En particular, se realiza un establecimiento de la comunicación DTLS basado en certificado mutuo, donde un cliente y un servidor poseen un par de claves públicas-privadas efímeras e intercambian las claves públicas durante el establecimiento de la comunicación. Estas claves públicas se utilizan para crear un secreto maestro previo, que a su vez se utiliza para generar un secreto maestro mediante una función pseudoaleatoria.

EXALTED: "WP5 - Security, Authentication & Provisioning. Deliverable 5.1 Security and Provisioning Solutions se refiere a la arquitectura de seguridad para las redes LTE-M en el ámbito del proyecto EXALTED.

Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema

Una de estas arquitecturas del 3GPP es la arquitectura de autenticación genérica (GAA), que es un complejo de estándares que se describe, por ejemplo, en 3GPP TS 33.919 (titulado "3G Security; Generic Authentication Architecture (GAA); System description", actualmente se puede recuperar en http://www.3gpp.org/ftp/Specs/html-info/33919.htm).

La arquitectura de arranque genérica (GBA) es un estándar del 3GPP definido en 3GPP TS 33.220 (titulado "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)", actualmente se puede recuperar en http://www.3gpp.org/ftp/specs/html-info/33220.htm). El GBA forma parte del complejo de estándares llamado GAA (véase más arriba).

El GBA es un estándar que permite derivar un secreto compartido (de arranque) a partir de la asociación de seguridad existente entre una red móvil y una tarjeta SIM. Se trata de un elemento de red llamado función de servidor de arranque (BSF). En otras palabras, el GBA aprovecha la seguridad de una tarjeta SIM (UICC) para autenticar equipos móviles y luego derivar material clave para aplicaciones de propósito general.

El GBA se puede utilizar ventajosamente para proporcionar alta seguridad en la comunicación entre un cliente y el servidor, lo que permite gestionar, controlar y, en general, comunicarse de forma remota con un dispositivo de una forma de alta seguridad. En particular, se utiliza el GBA (o una arquitectura parecida al GBA) para permitir una comunicación segura con el dispositivo (que, según un aspecto de la presente divulgación, puede ser un dispositivo M2M), siendo dicha comunicación entre un servidor y un cliente, estando asociado el cliente con el dispositivo, y en el que esta comunicación se realiza para gestionar el dispositivo y/o los servicios proporcionados por (o por medio de) el dispositivo, lo que permite una gestión segura de ese dispositivo y/o los servicios proporcionados por (o por medio de) el dispositivo. De esta manera, el dispositivo y/o los servicios proporcionados por (o por medio de) el dispositivo se pueden gestionar de forma segura y eficaz de forma remota por medio de un servidor remoto.

El GBA se ha desarrollado principalmente para asegurar la radiodifusión móvil (p. ej., televisión de pago y equivalentes). De hecho, los estándares para el servicio de multidifusión y radiodifusión multimedia (MBMS) se basan en GBA. De forma similar, el perfil de tarjeta inteligente del conjunto de servicios habilitadores de radiodifusión móvil (BCAST) de Open Mobile Alliance (OMA) se basa en GBA. Hasta la fecha, la mayor parte del número limitado de despliegues del GBA en el mundo ha sido para la radiodifusión móvil. El GBA también se ha estandarizado como una

característica opcional junto con los servicios de presencia y dentro de diversos servicios de "identidad federada" (p. ej., Liberty Alliance, OpenID). En general, se entiende que el GBA se ha diseñado para su uso en dispositivos móviles, tales como teléfonos móviles, portátiles, ordenadores, y muchas de las características diseñadas se han provisto teniendo esto en cuenta.

Se ha propuesto una variante del GBA, llamada "inserción de GBA", para asegurar un mensaje entre un cliente y un servidor DM en el contexto de seguridad de gestión de dispositivos OMA. La gestión de dispositivos OMA está diseñada específicamente para la gestión de dispositivos móviles tales como teléfonos móviles, tabletas, ordenadores, etc.

Un documento estándar reciente diferente (TS 102 690) meramente menciona, en el contexto de las comunicaciones M2M, el uso de un GBA estándar para asegurar las comunicaciones entre una capa de servicio de dispositivo/puerta de enlace y una capa de servicio de red.

Existen algunas alternativas para identificar/autenticar a un usuario/dispositivo móvil en un servicio. Todas estas alternativas son más sencillas que utilizar GBA. Por ejemplo, los operadores móviles y los proveedores de servicios pueden utilizar el enriquecimiento de encabezados WAP.

De forma alternativa, el proveedor de servicios puede solicitar al usuario que introduzca su número de teléfono, enviar una contraseña de un solo uso por SMS a ese número de teléfono y pedirle al usuario que lea el SMS e introduzca la contraseña. Todas estas alternativas ya funcionan bien con dispositivos y operadores móviles, por lo que los proveedores de servicios las utilizan, aunque no son tan seguras como GBA.

Además, muchos proveedores de servicios prefieren ofrecer servicios a una amplia gama de dispositivos móviles, muchos de los cuales no contienen una tarjeta SIM (p. ej., PC, portátiles, tabletas solo con conexión wifi, etc.). Dado que GBA depende de una tarjeta SIM/UICC para funcionar, no ha habido interés en utilizarlo.

Una seguridad sólida no es posible con las alternativas actuales, tales como un PIN introducido por el usuario o un mensaje de arranque enviado por SMS. Estas alternativas no serían viables o no proporcionarían el nivel de seguridad requerido. En primer lugar, es posible que no haya un usuario cerca para introducir un PIN (ya que la mayoría de los dispositivos M2M funcionan independientemente de la intervención humana). En segundo lugar, es probable que el proveedor de servicios desee una seguridad sólida (p. ej., porque los dispositivos M2M pueden incluir infraestructura crítica), mientras que el arranque basado en PIN tiene una seguridad más débil. En tercer lugar, si un PIN o un arranque basado en SMS sale mal (el servidor se conecta a un cliente equivocado, el cliente se conecta a un servidor equivocado o hay un hombre en el medio), entonces es probable que el usuario se dé cuenta, se queje y lo arregle, mientras que es poco probable que un dispositivo M2M se dé cuenta y se queje, por lo que puede verse comprometido permanentemente. Ninguno de los dos es especialmente práctico a través de los procedimientos existentes. Por ejemplo, la gestión de dispositivos OMA utiliza la inserción de GBA para asegurar un mensaje entre un cliente y un servidor DM, y no hay explicación de cómo se podría usar o incluso modificar una arquitectura parecida para gestionar el dispositivo. Además, como se ha mencionado anteriormente, la gestión de dispositivos OMA no es compatible para su uso con un dispositivo M2M, como se analiza anteriormente. Esto es particularmente cierto para dispositivos M2M simples y de bajo coste, tales como sensores simples, conmutadores, rastreadores de bajo coste, etc. Además, el documento estándar mencionado anteriormente utiliza un GBA estándar para asegurar las comunicaciones entre una capa de servicio de dispositivo/puerta de enlace y una capa de servicio de red. Así, la comunicación no se utiliza en comunicaciones relacionadas con la gestión de dispositivos/servicios y no está claro, en base a las observaciones realizadas anteriormente, cómo se podría utilizar o incluso modificar una arquitectura parecida para gestionar el dispositivo desde el servidor. Además, por los motivos mencionados anteriormente, la gestión de dispositivos OMA y el documento estándar son incompatibles, y una combinación de inserción de GBA para la gestión de dispositivos OMA con el documento estándar no es viable, ya que daría como resultado un protocolo de gestión de dispositivos incorrecto (es decir, que no es adecuado para dispositivos M2M, en particular dispositivos M2M simples), y un esfuerzo muy laborioso para hacer que ambos sean compatibles y eliminar los elementos que son redundantes.

La OMA ha definido un protocolo de baja complejidad para gestionar (así como interactuar con) dispositivos M2M y gestionar los servicios proporcionados por dispositivos M2M (p. ej., control remoto de sensores o máquinas conectadas). Este protocolo se llama LWM2M y se describe detalladamente en

http://technical.openmobilealliance.org/Technical/release_program/lightweightM2M_v1_0.aspx

Este protocolo se ejecuta sobre el protocolo CoAP (análogo a http), más específicamente CoAP sobre DTLS (coaps), que es análogo a http sobre TLS (https). Sin embargo, coaps requiere que se proporcione una asociación segura entre un dispositivo y un servidor de red (servidor DM) al tiempo que no proporciona los medios sólidos para proporcionar dicha asociación desde cero.

Un aspecto de seguridad del OMA LWM2M se define en la versión candidata 1.0 de las especificaciones técnicas del protocolo de máquina a máquina de baja complejidad - 10 de diciembre de 2013 (OMA-TS-LightweightM2M-V1_0-20131210-C).

Además, existen dos protocolos, el primero llamado DTLS definido en RFC 6347 (titulado "Datagram Transport Layer Security Version 1.2"; actualmente se puede recuperar en http://tools.ietf.org/html/rfc6347); el segundo llamado CoAP

definido en draft-ietf-core-coap-18 (titulado "Constrained Application Protocol (CoAP)"; actualmente se puede recuperar en http://datatracker.ietf.org/doc/draft-ietf-core-coap/). Ambos protocolos se utilizan actualmente en LWM2M. CoAP es todavía solo un borrador del IETF (no un RFC completo), y la versión 1.2 de DTLS también es comparativamente nueva (enero de 2012): las versiones de TLS a menudo han existido como RFC durante varios años antes de recibir una adopción generalizada.

La seguridad del canal con el protocolo de datagramas de usuario (UDP) para [COAP] se define en la seguridad de la capa de transporte de datagramas (DTLS) [RFC6347], que es el equivalente de TLS v1.2 [RFC5246] para HTTP y utiliza un subconjunto de los conjuntos de cifrado definidos en TLS. (Se refiere al registro de los conjuntos de cifrado TLS http://www.iana.org/assignments/tls-parameters/tls-parameters.xml) La enlace de DTLS para CoAP se define en la sección 9 de [CoAP]. DTLS es una solución de seguridad basada en sesiones de larga duración para UDP. Proporciona un establecimiento de la comunicación seguro con generación de claves de sesión, autenticación mutua, integridad de datos y confidencialidad.

El material para claves utilizado para asegurar el intercambio de información dentro de una sesión DTLS se puede obtener utilizando uno de los modos de arranque definidos en la sección 5.1.2 Modos de arranque de OMA LWM2M. Los formatos del material para claves transportado en las instancias de objeto de seguridad LWM2M se definen en el apéndice E.1.1.

También existe un protocolo de autenticación implícita HTTP, que se define en RFC 3310 (titulado "Hypertext Transfer protocol (HTTP) Digest Authentication using Authentication and Key Agreement (AKA)", que actualmente se puede recuperar en http://www.ietf.org/rfc/rfc3310.txt).

El grupo de especificaciones GAA TS 33.222 (titulado "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)") define un planteamiento general para la clave precompartida TLS (TLS-PSK, RFC 4279). Actualmente se puede recuperar en http://www.3gpp.org/ftp/Specs/html-info/33222.htm). Por ejemplo, véase especialmente la sección 5.4.

En particular, con referencia a GBA, la especificación 3GPP TS 33.220 define los componentes e interfaces que se muestran en la figura 1. Estos se describen además como:

NAF 122, la "función de aplicación de red" es un componente del lado del servidor de una aplicación que se asegurará mediante GBA.

BSF, "función de servidor de arranque", 130 es un componente del lado del servidor, que obtiene vectores de autenticación a partir del HLR/HSS 140 y envía un desafío al dispositivo móvil, "UE", 110 durante el protocolo GBA. Tras una autenticación satisfactoria, deriva el secreto compartido.

HLR/HSS 140, el "registro de ubicación local" o "sistema de abonado local", es el sistema 3GPP existente que almacena detalles de abono y credenciales (K e IMSI) para cada tarjeta SIM (UICC) emitida por un operador de telefonía móvil. Puede ser "compatible con GBA" (para que almacene detalles del abono de un usuario de GBA) o puede ser un componente heredado.

UE, el "equipo de usuario", 110 es un dispositivo móvil que contiene una tarjeta SIM (UICC). El UE 110 admite una aplicación cliente que se comunica con la NAF 122, así como un servicio que interactúa con la UICC, se comunica con la BSF 130 y deriva el secreto compartido antes de pasarlo a la aplicación cliente. Este servicio se denomina (de manera algo confusa) "servidor GAA" en TR 33.905 (titulado "Recommendations for Trusted Open Platforms", actualmente se puede recuperar en http://www.3gpp.org/ftp/specs/htmlinfo/33905.htm).

Ua 150 es la interfaz entre el dispositivo móvil (UE) 110 y la función de aplicación de red (NAF) 120.

Ub 160 es la interfaz entre el dispositivo móvil (UE) 110 y la función de servidor de arranque (BSF) 130. Esto se especifica en detalle en TS 24.109 (titulado "Bootstrapping interface (Ub) 160 and network application function interface (Ua) 150; Protocol details", actualmente se puede recuperar en http://www.3gpp.org/ftp/Specs/html-info/24109.htm).

Zh/Zh' 180 es la interfaz entre la BSF 130 y el HSS o HLR 140. La interfaz Zh 180 se utiliza con un HSS 140 que es "compatible con GBA". La interfaz Zh' 180 se utiliza con un HLR o HSS 140 heredado. Las interfaces Zh y Zh' 180 se especifican en detalle en TS 29.109 (titulado "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on Diameter protocol; Stage 3", actualmente se puede recuperar en http://www.3gpp.org/ftp/Specs/html-info/29109.htm) y TS 29.229 (titulado "Cx and Dx interfaces based on the Diameter protocol; protocol details", actualmente se puede recuperar en http://www.3gpp.org/ftp/Specs/html-info/29229.htm).

Zn 170 es la interfaz entre la NAF 122 y la BSF 130: puede utilizar un protocolo de servicios web (SOAP sobre http) o el protocolo del Diámetro (RFC 3588). Esto se especifica en detalle en TS 29.109 (véase más arriba).

Existen algunos otros componentes e interfaces definidos dentro de los estándares GAA, pero no se describen en detalle aquí.

Existen varias versiones diferentes de GBA definidas en los estándares. Los tipos de GBA pueden incluir GBA-ME,

GBA-U, GBA-SIM, etc. Es posible que la versión denominada "GBA-ME" no requiera personalizaciones especiales de la UICC, a menos que la UICC contenga una SIM 3G (una USIM). Sin embargo, se pueden utilizar otras versiones. Puede que sea necesario utilizar la variante 2G del GBA (que utiliza una SIM en lugar de una USIM).

Compendio de la invención

Según un primer aspecto, se proporciona un procedimiento para comunicarse de forma segura con un dispositivo de máquina a máquina, M2M, que comprende las etapas de:

compartir un secreto o los datos derivados del secreto entre el dispositivo M2M y un servidor;

establecer una conexión entre el dispositivo M2M y el servidor;

utilizar el secreto compartido o los datos derivados del secreto compartido para establecer el material criptográfico tanto en el dispositivo M2M como en el servidor; y

asegurar la comunicación entre el dispositivo M2M y el servidor con un protocolo criptográfico que utiliza el material criptográfico establecido, en el que el material criptográfico es irrecuperable a partir del secreto compartido o de los datos derivados únicamente del secreto compartido.

Por lo tanto, se puede abrir una conexión o canal de comunicación que proporcione seguridad o autenticación débil o nula y luego utilizarse para iniciar un protocolo de seguridad que permita un mayor nivel de seguridad o autenticación. Por ejemplo, la conexión puede utilizar un punto de acceso wifi no seguro. Si bien esta conexión no tiene que ser segura, puede utilizarse para establecer o autenticar material (p. ej., claves) de modo que el material criptográfico solo esté disponible para el dispositivo M2M y el servidor. El material criptográfico no puede ser recuperado por ninguna otra parte, incluso si esa parte conoce el secreto compartido. Esto proporciona el secreto directo perfecto.

Opcionalmente, la etapa de utilizar el secreto compartido o los datos derivados del secreto compartido para establecer el material criptográfico puede comprender además las etapas de:

el dispositivo M2M genera u obtiene una clave pública;

el servidor autentica la clave pública del dispositivo M2M utilizando el secreto compartido o los datos derivados del secreto compartido; y

el servidor deriva el material criptográfico a partir de la clave pública del dispositivo M2M. La clave pública puede tener una clave privada correspondiente. El dispositivo M2M puede proporcionar una nueva clave pública, recuperar una clave pública almacenada u obtener la clave de otro lugar, por ejemplo.

Ventajosamente, la etapa de autenticar la clave pública del dispositivo M2M puede emplear una comunicación entre un servidor de arranque y el dispositivo M2M. O una comunicación entre el servidor y el servidor de arranque. Por ejemplo, el dispositivo M2M puede pasar una clave pública o un certificado a una BSF como parámetro dentro del protocolo de arranque. La BSF puede pasar la clave pública del dispositivo a una NAF como parte de un GUSS o USS, por ejemplo.

Opcionalmente, la etapa de utilizar el secreto compartido o los datos derivados del secreto compartido para establecer el material criptográfico puede comprender además las etapas de:

el servidor genera u obtiene una clave pública;

el dispositivo M2M autentica la clave pública del servidor utilizando el secreto compartido o los datos derivados del secreto compartido; y

el dispositivo M2M obtiene el material criptográfico a partir de la clave pública del servidor. La clave pública puede tener una clave privada correspondiente. El servidor puede proporcionar una nueva clave pública, recuperar una clave pública almacenada u obtener la clave de otro lugar, por ejemplo.

Ventajosamente, la etapa de autenticar la clave pública del servidor puede emplear una comunicación entre un servidor de arranque y el dispositivo M2M, o una comunicación entre el servidor y el servidor de arranque. Por ejemplo, la BSF puede pasar la clave pública o el certificado del servidor (o una clave pública de autoridad utilizada para firmar el certificado del servidor) al dispositivo M2M como parámetro dentro del protocolo de arranque. La BSF puede crear un certificado para la NAF, que la NAF puede utilizar cuando se comunica con el dispositivo, por ejemplo.

Ventajosamente, la etapa de utilizar el secreto compartido o los datos derivados del secreto compartido para establecer el material criptográfico tanto en el dispositivo M2M como en el servidor puede comprender además las etapas de:

el dispositivo M2M genera u obtiene una clave pública y una clave privada correspondiente;

el servidor genera u obtiene una clave pública y una clave privada correspondiente;

el dispositivo M2M autentica la clave pública del servidor utilizando el secreto compartido o los datos derivados del secreto compartido;

el servidor autentica la clave pública del dispositivo M2M utilizando el secreto compartido o los datos derivados del secreto compartido;

el dispositivo M2M deriva el material criptográfico a partir de la clave pública del servidor y la clave privada del dispositivo M2M; y

el servidor deriva el material criptográfico a partir de la clave pública del dispositivo M2M y la clave privada del servidor. En esta realización, el dispositivo M2M y el servidor generan cada uno un par de claves pública/privada, cada uno usa el secreto compartido para autenticar la clave pública del otro. Cada uno utiliza su propia clave privada y la clave pública del otro para derivar el material criptográfico. Este es un mecanismo que impide que el material criptográfico se derive u obtenga simplemente a partir del conocimiento de las claves públicas y el secreto compartido original.

Preferiblemente, el material criptográfico pueden ser claves de sesión para proporcionar un secreto directo perfecto. Esto significa que, si el secreto se ve comprometido, los mensajes antiguos o históricos no necesariamente están sujetos a una recuperación no autorizada.

Preferiblemente, el protocolo criptográfico puede ser TLS, SSL o seguridad de la capa de transporte de datagramas, DTLS. Estos pueden tomar la forma de un protocolo de acuerdo de claves de Diffie-Hellman de curva elíptica, por ejemplo.

Opcionalmente, el secreto compartido puede generarse o almacenarse dentro del dispositivo M2M y el secreto compartido o los datos derivados del secreto compartido se envían al servidor. El secreto compartido puede proveerse previamente o generarse en el primer encendido, por ejemplo.

Opcionalmente, el procedimiento puede comprender además la etapa de que el servidor autentica el secreto compartido. En algunas realizaciones, el servidor puede autenticar el secreto compartido (o el material derivado).

Opcionalmente, el secreto compartido puede generarse o almacenarse dentro del servidor y el secreto compartido o los datos derivados a partir del secreto compartido se envían al dispositivo M2M.

Opcionalmente, el procedimiento puede comprender además la etapa de que el dispositivo M2M autentica el secreto compartido. Opcionalmente, tanto el dispositivo M2M como el servidor pueden autenticar el secreto compartido (o el material derivado) generado o almacenado en la otra entidad.

Opcionalmente, los datos derivados del secreto compartido se pueden obtener aplicando una función hash u otra función de derivación de clave fija al secreto compartido. Se pueden utilizar otras técnicas de derivación.

Opcionalmente, el servidor puede ser un servidor de gestión de dispositivos, un servidor de arranque de gestión de dispositivos, un servidor de M2M de baja complejidad, LWM2M, un servidor de arranque LWM2M o una función de aplicación de red, NAF u otra entidad.

Opcionalmente, el servidor puede ser una función de servidor de arranque, BSF.

Opcionalmente, el procedimiento puede comprender además la etapa de autenticar el secreto compartido o utilizar el secreto compartido para autenticar uno o ambos, el dispositivo M2M y el servidor.

Ventajosamente, la conexión establecida entre el dispositivo M2M y el servidor puede no ser segura o tener solo una seguridad débil.

Ventajosamente, la comunicación segura entre el dispositivo M2M y el servidor se realiza a través de la conexión. En algunas realizaciones, la comunicación segura se realiza a través de una conexión separada.

Preferiblemente, la etapa de asegurar la conexión entre el dispositivo M2M y el servidor comprende además proporcionar mensajes de arquitectura de arranque genérico, GBA, o de información de inserción de GBA, GPI, a través de la conexión o a través de una conexión separada.

Opcionalmente, el secreto compartido puede utilizarse para establecer, proteger, respaldar o autenticar uno o más de un certificado, un certificado digital, un certificado autofirmado o un certificado firmado por una autoridad certificadora desconocida o no verificable. Se puede utilizar otro material. La clave privada puede estar en manos del dispositivo M2M. La clave privada puede estar en manos del servidor. Tanto el dispositivo M2M como el servidor pueden contener cada uno una clave privada, y cada clave pública o certificado correspondiente se establece, protege, respalda o autentica utilizando el secreto compartido, por ejemplo.

Opcionalmente, el secreto compartido puede utilizarse para establecer, proteger, respaldar o autenticar una clave o certificado de autoridad. Luego, la clave de autoridad se utiliza para firmar, respaldar o autenticar una clave pública o un certificado para el dispositivo y/o servidor. Por ejemplo, el secreto compartido se puede utilizar para distribuir un

certificado de autoridad certificadora (CA) para una CA previamente desconocida.

Opcionalmente, el secreto compartido se puede utilizar para verificar que una clave pública o un certificado sigue siendo válido (p. ej., no ha caducado ni ha sido revocado), incluida una clave o certificado de autoridad. O el secreto compartido puede utilizarse para autenticar un certificado o una clave pública actualizada, incluida una clave o certificado de autoridad. Por ejemplo, el secreto compartido se puede usar de esta manera cuando el dispositivo no tiene acceso a un reloj exacto (por lo que no puede verificar el tiempo de caducidad), o cuando el dispositivo no puede recuperar información de revocación como CRL, o el secreto compartido se puede usar para actualizar o reemplazar los certificados de CA.

Preferiblemente, el secreto compartido puede configurarse para que caduque en un momento predeterminado. Por lo tanto, no es necesario que el material caduque activamente.

Opcionalmente, el servidor puede generar un identificador de transacción configurado para caducar en un momento predeterminado y además, en el que el tiempo de caducidad del secreto compartido se corresponde con el tiempo de caducidad del identificador de transacción.

Ventajosamente, el procedimiento puede comprender además la etapa de obtener información que indica el tiempo actual a partir de una fuente de tiempo fiable. Por lo tanto, se puede basar en esto para determinar si el secreto compartido ha caducado o no.

Preferiblemente, la información que indica el tiempo actual se puede obtener a partir de mensajes de la fuente de tiempo fiable asegurada mediante GBA.

Según un segundo aspecto, se proporciona un sistema que comprende:

un servidor;

uno o más dispositivos móviles o de máquina a máquina, M2M; y

lógica configurada para:

compartir un secreto o los datos derivados del secreto entre el uno o más dispositivos M2M y el servidor;

establecer una conexión entre el uno o más dispositivos M2M y el servidor;

utilizar el secreto compartido o los datos derivados del secreto compartido para establecer el material criptográfico tanto en el dispositivo M2M como en el servidor; y

comunicación segura entre el dispositivo M2M y el servidor con un protocolo criptográfico que utiliza el material criptográfico establecido, en el que el material criptográfico es irrecuperable a partir del secreto compartido o de los datos derivados únicamente del secreto compartido.

Opcionalmente, el uno o más dispositivos M2M pueden configurarse para generar u obtener una clave pública y una clave privada correspondiente, y en el que el servidor está además configurado para generar u obtener una clave pública y una clave privada correspondiente; el uno o más dispositivos M2M están configurados para autenticar la clave pública del servidor utilizando el secreto compartido o los datos derivados del secreto compartido;

el servidor está configurado para autenticar la clave pública del uno o más dispositivos M2M utilizando el secreto compartido o los datos derivados del secreto compartido;

el uno o más dispositivos M2M están configurados para derivar el material criptográfico a partir de la clave pública del servidor y la clave privada del dispositivo M2M; y

el servidor está configurado para derivar el material criptográfico a partir de la clave pública del dispositivo M2M y la clave privada del servidor.

Los procedimientos descritos anteriormente pueden implementarse como un programa informático que comprende instrucciones de programa para hacer funcionar un ordenador. El programa informático puede almacenarse en un medio legible por ordenador.

El sistema informático puede incluir un procesador tal como una unidad central de procesamiento (CPU). El procesador puede ejecutar lógica en forma de programa de software. El sistema informático puede incluir una memoria que incluye un medio de almacenamiento volátil y no volátil. Se puede incluir un medio legible por ordenador para almacenar la lógica o las instrucciones del programa. Las diferentes partes del sistema pueden conectarse mediante una red (p. ej., redes inalámbricas y cableadas. El sistema informático puede incluir una o más interfaces. El sistema informático puede contener un sistema operativo adecuado, tal como por ejemplo UNIX, Windows (RTM) o Linux.

La invención se define en las reivindicaciones.

Breve descripción de las figuras

La presente invención se puede poner en práctica de varias maneras y a continuación se describirán realizaciones únicamente a modo de ejemplo y en referencia a los dibujos adjuntos, en los que:

la figura 1 muestra un diagrama esquemático de componentes e interfaces con los que se puede utilizar GBA;

la figura 2 muestra un diagrama esquemático de un ejemplo de una arquitectura que puede usarse según la presente invención, en particular cuando se utiliza GBA;

la figura 3 muestra un diagrama de flujo ejemplar de comunicaciones intercambiadas dentro de la arquitectura ejemplar de la figura 2;

la figura 4 muestra un diagrama esquemático de un ejemplo de una arquitectura alternativa que puede usarse según la presente invención, en particular cuando se utiliza una arquitectura de arranque genérica (GBA);

la figura 5 muestra un diagrama esquemático de un servidor de gestión de dispositivos (DM) en comunicación con un dispositivo máquina a máquina (M2M);

la figura 6 muestra un diagrama esquemático de un sistema y procedimiento para iniciar comunicaciones entre el servidor DM y el dispositivo M2M de la figura 5;

la figura 7 muestra un diagrama esquemático de otro sistema y procedimiento para iniciar comunicaciones entre el servidor DM y el dispositivo M2M de la figura 5;

la figura 8 muestra un diagrama de flujo de un procedimiento para comunicarse de forma segura con un dispositivo M2M; y

la figura 9 muestra un diagrama esquemático de un sistema para implementar el procedimiento de la figura 8.

Cabe destacar que las figuras se ilustran por simplicidad y no necesariamente están dibujadas a escala. Las características parecidas se proporcionan con los mismos números de referencia.

Descripción detallada de las realizaciones preferidas

Un dispositivo puede comunicarse de forma segura con un servidor. El dispositivo puede ser un dispositivo máquina a máquina (M2M), o un dispositivo equivalente (p. ej., un dispositivo, un dispositivo de comunicación genérico o específico, incluido uno o más módulos que pueden proporcionar capacidades M2M).

Los aspectos de la arquitectura de autenticación genérica (GAA) y la arquitectura de arranque genérica (GBA) se identifican en el apartado anterior "Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema". En particular, la arquitectura específica en la que se puede basar el procedimiento y el sistema es el GBA.

La arquitectura de arranque genérica (GBA) utiliza asociaciones de seguridad existentes entre una red (p. ej., una red móvil) y una tarjeta (p. ej., una tarjeta SIM o UICC) para derivar una clave que se puede utilizar en la comunicación segura entre el cliente y el servidor. En consecuencia, si el dispositivo está asociado con dicha tarjeta, así como con el cliente, el procedimiento puede utilizar ventajosamente el GBA para derivar los elementos de seguridad (p. ej., un secreto compartido) que permiten que el cliente asociado con el dispositivo se comunique de forma segura con el servidor. En consecuencia, el dispositivo podría adaptarse ventajosamente para que esté asociado con la tarjeta y el cliente y utilice el GBA para derivar los elementos de seguridad para una comunicación segura con el servidor. Además, como el GBA se basa en estándares, el impacto de las modificaciones necesarias puede ser relativamente limitado y la solución global sería muy atractiva (en particular, para los usuarios/propietarios de M2M, así como para los operadores de redes y/o proveedores de servicios).

Los dispositivos M2M son diferentes de los dispositivos móviles para los que se diseñó originalmente la gestión de dispositivos OMA (tales como teléfonos móviles, ordenadores portátiles, ordenadores, como se explica en el apartado anterior "Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema"), y el uso de GBA (en cualquiera de sus versiones) con M2M no es una implementación sencilla.

Se ha propuesto una variante del GBA, llamada "inserción de GBA" para asegurar un mensaje entre un cliente y un servidor DM en el contexto de seguridad de gestión de dispositivos OMA, y se identifica en el apartado "Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema" anterior. Cabe señalar que, aunque la inserción de GBA y GBA están relacionados, no es trivial utilizar GBA en lugar de inserción de GBA (y viceversa). Esto se debe a que estas dos arquitecturas tienen algunas diferencias importantes. Primero, en GBA el dispositivo tiene que ponerse en contacto con la BSF para solicitar un RAND y un AUTN (y usarlo para derivar una Ks_local). Por el contrario, en la inserción de GBA, el cliente no tiene que hablar con la BSF: simplemente recibe un mensaje preparado por la BSF. Además, en GBA no es necesario modificar la interfaz Ua. En la inserción de GBA, la interfaz Ua debe modificarse de alguna manera para llevar el mensaje de inserción o se debe añadir una nueva

interfaz. En consecuencia, la inserción de GBA no se puede utilizar con un protocolo de aplicación arbitrario. Para la inserción de GBA, el protocolo de aplicación tiene que ser "compatible con GBA" en algún sentido (p. ej., para que pueda llevar los mensajes con información de inserción de GBA (GPI)). En GBA, la Ks_local se puede utilizar para derivar varias Ks_NAF diferentes (p. ej., para servidores de aplicaciones diferentes). En la inserción de GBA, solo una NAF puede utilizar/basarse en la Ks_local. En consecuencia, la inserción de GBA es algo menos eficaz que el GBA.

La información de inserción de GBA se describe en el 3GPP TS 33.223, sección 5.2.1. La codificación se define en la sección 5.3.5. Véase en particular la tabla 5.2.1.1 y la figura 5.3.5.1 en 3GPP TS 33.223 V12.0.0 (2013-12) que se puede encontrar: http://www.3gpp.org/ftp/Specs/archive/33_series/33.223/33223-c00.zip

Además, como se analiza anteriormente, los dispositivos M2M tienen capacidades muy limitadas (p. ej., computación, comunicación, duración, etc.) y estas limitaciones hacen que su gestión sea más compleja y difícil de implementar de forma sencilla. El GBA requiere varios interfaces y componentes que son difíciles de implementar con M2M (para ver ejemplos y descripciones de estas interfaces y componentes, consulte las secciones siguientes).

Para gestionar de forma más eficaz y segura el dispositivo y/o los servicios proporcionados por (o por medio de) el dispositivo, estas interfaces y componentes deben modificarse o en cualquier caso adaptarse para que puedan funcionar de forma adecuada y eficaz con dispositivos M2M.

Por ejemplo, llevar la interfaz Ub (y el protocolo asociado) a través de dispositivos M2M limitados es muy difícil. Por ejemplo, la interfaz Ub estándar utiliza HTTP y autenticación implícita HTTP. La razón probable para esto es que, como se ha mencionado anteriormente, el GBA se diseñó teniendo en mente los dispositivos móviles, tales como los teléfonos móviles. Entonces, dado que todos los teléfonos usan HTTP y, por lo tanto, todos tienen una pila HTTP, HTTP fue el protocolo más fácil de utilizar para la interfaz Ub. Sin embargo, esto no es cierto para los dispositivos M2M. Por ejemplo, según el protocolo de M2M de baja complejidad (LWM2M) (véase a continuación para más detalles), se utiliza un protocolo llamado CoAP en los dispositivos M2M, justamente porque es una alternativa más sencilla/eficaz al HTTP.

De forma alternativa, esta interfaz Ub podría tunelizarse, por ejemplo, por medio de otra interfaz (p. ej., la Ua), de modo que se pueda simplificar el sistema.

Además, parece muy difícil construir todos los componentes necesarios (p. ej., servidor GAA, interfaces) en un dispositivo M2M con capacidad limitada. Por ejemplo, las limitaciones de espacio físico y virtual, así como las limitaciones computacionales, crean problemas considerables para construir los componentes necesarios. Además, es muy difícil tener una o más interfaces entre las aplicaciones M2M y una tarjeta en el dispositivo, tal como una UICC. Esto se debe, por ejemplo, al hecho de que la mayoría de los módems M2M no admiten las interfaces de bajo nivel requeridas. En general, la integración global de las interfaces y componentes necesarios del GBA con un dispositivo M2M parece muy difícil. Una solución posible, pero no óptima, podría ser proveer previamente los dispositivos M2M (p. ej., tener los dispositivos M2M ya diseñados y/o fabricados con los componentes e interfaces necesarios) y los elementos asociados necesarios para el uso de GBA (p. ej., la tarjeta con capacidad de interactuar con el dispositivo M2M) de modo que se pudiera utilizar el GBA. Hasta la fecha, ningún dispositivo M2M está provisto previamente con estas características.

Además, como se indica anteriormente, el GBA no se usa ampliamente. Existen otros motivos por los que el GBA no se utiliza ampliamente. Por ejemplo, el uso de GBA requiere soporte en el dispositivo, en la red (p. ej., BSF, véase a continuación) y por servicios individuales (que pueden desplegarse, por ejemplo, mediante un operador de telefonía móvil o por otras partes). En el caso de uso preferido (radiodifusión móvil), también se requiere compatibilidad con la tarjeta SIM (ya que utiliza GBA-U). En consecuencia, la falta de coordinación y voluntad de actuar/cooperar entre las diversas partes involucradas en este despliegue (p. ej., fabricantes de dispositivos, operadores móviles, proveedores de servicios) ha bloqueado hasta ahora la implementación del GBA.

Por todos los motivos anteriores, se puede utilizar GBA (o una arquitectura parecida al GBA, por ejemplo, una variante y/o una versión adecuadamente modificada) que permita una comunicación segura con un dispositivo (en particular, un dispositivo M2M). La comunicación puede ser entre un servidor y un cliente, estando el cliente asociado con el dispositivo, y en el que esta comunicación puede realizarse para gestionar el dispositivo y/o los servicios proporcionados por (o por medio de) el dispositivo. Ello permite una gestión segura de ese dispositivo y/o de los servicios proporcionados por (o por medio de) el dispositivo y crea una combinación nueva e innovadora que produce un efecto sinérgico y proporciona muchas ventajas técnicas.

Por ejemplo, como ya se ha mencionado anteriormente, el GBA proporcionará un nivel de seguridad más alto y muy sólido para las comunicaciones relacionadas con la gestión de dispositivos/servicios con dispositivos M2M, que es un punto muy crítico e importante.

Otra ventaja, además o combinada con la sólida seguridad descrita anteriormente, es la automatización total. Además, un proveedor de servicios M2M no tiene el coste ni la complejidad de configurar sus propias soluciones de seguridad, ya que la solución puede ser proporcionada directamente por el operador móvil que implementa la solución descrita en esta solicitud. En particular, un proveedor de servicios no tiene que establecer una PKI, emitir certificados, precargar claves en los dispositivos, etcétera.

En consecuencia, el procedimiento puede comprender además que el aprovisionamiento de la comunicación segura esté basado en una asociación de seguridad entre una red y una tarjeta, estando asociada la tarjeta con el dispositivo. Por ejemplo, la tarjeta puede estar integrada dentro del dispositivo (p. ej., soldada en el dispositivo) o proporcionada al dispositivo por medio de una conexión adecuada. En general, la tarjeta puede asociarse de cualquier manera adecuada para que exista una asociación entre la tarjeta y el dispositivo. La red puede ser una red móvil o cualquier red equivalente, mientras que la tarjeta puede ser una tarjeta SIM, una UICC o cualquier tarjeta asociada a la red. El procedimiento puede comprender además derivar un secreto compartido basado en la asociación de seguridad. El procedimiento puede comprender además proporcionar al cliente y al servidor el secreto compartido para permitir la comunicación segura. El servidor puede ser un servidor adaptado para gestionar el dispositivo (p. ej., gestionar de forma remota el dispositivo, enviar actualizaciones, transferir información hacia y desde el dispositivo, controlar parámetros del dispositivo, etc.) y para gestionar los servicios proporcionados por el dispositivo (p. ej., el dispositivo se utiliza para encender/apagar y/o atenuar las luces de la calle). El secreto compartido puede ser una clave y/o una disposición de seguridad parecida.

El procedimiento puede comprender además autenticación entre el cliente y el servidor. La autenticación puede basarse en el secreto compartido. La autenticación se puede realizar por medio de un componente de autenticación. La autenticación puede realizarse por medio de una primera autenticación entre el cliente y un componente de autenticación y una segunda autenticación entre el servidor y el componente de autenticación. El cliente y el servidor pueden autenticarse de forma independiente mediante un componente de autenticación. Como resultado de que el componente de autenticación autentica al cliente y al servidor, tanto el cliente como el servidor pueden compartir el secreto compartido. La autenticación puede realizarse por medio del secreto compartido. El secreto compartido puede compartirse entre el cliente y el servidor. De forma alternativa, el secreto compartido puede compartirse entre el cliente, el servidor y el componente de autenticación. La autenticación puede resultar implícitamente de que el cliente, el servidor y el componente de autenticación compartan el secreto compartido. El procedimiento puede comprender además derivar un segundo secreto compartido basándose en el secreto compartido, siendo compartido el segundo secreto compartido entre el cliente y el servidor. Este segundo secreto compartido puede usarse entonces para la autenticación como se analiza anteriormente.

La obtención del secreto compartido en el cliente puede basarse en un identificador asociado con un componente de autenticación del servidor. El secreto compartido se puede obtener en el servidor desde el componente de autenticación. La obtención del secreto compartido en el servidor se obtiene en base a un identificador asociado con el secreto compartido. El identificador lo genera el componente de autenticación. El identificador puede ser proporcionado al servidor por parte del cliente.

Se puede utilizar el protocolo OMA LWM2M para gestionar (así como interactuar con) dispositivos M2M y gestionar los servicios proporcionados por dispositivos M2M (como se describe en el apartado "Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema"). Sin embargo, se pueden usar otros protocolos de gestión de dispositivos o el procedimiento y el sistema se pueden extender a otros servicios M2M (por ejemplo, asegurar la entrega de SMS binarios).

El GBA podría utilizarse ventajosamente junto con LWM2M para, por ejemplo, establecer claves para LWM2M, mientras que al mismo tiempo LWM2M y los procedimientos especificados en el mismo podrían utilizarse para transportar y/o llevar cualquier mensaje y/o comunicación que esté relacionada con el GBA. Por ejemplo, esto se puede hacer mediante el uso de túneles específicos (p. ej., Ub) o mensajes con información de inserción de GBA (GPI). El uso de GBA junto con LWM2M crea una combinación nueva e innovadora que produce un efecto sinérgico y proporciona muchas ventajas técnicas. Por ejemplo, permite abordar muchos más dispositivos de gama baja, tales como los dispositivos M2M. Esto se debe, por ejemplo, al uso de un protocolo de gestión de dispositivos que está adecuadamente optimizado para M2M, en lugar de uno reutilizado desde el espacio del consumidor (p. ej., OMA DM v1, TR-069). Este protocolo optimizado se puede utilizar para transportar mensajes GBA, lo que evita la necesidad de una pila HTTP separada, y para gestionar parámetros GBA (identificadores de dispositivo y aplicación, duraciones, procedimientos de derivación de claves, etc.). Además, cuando van acompañados de sistemas de red apropiados para proporcionar el encaminamiento y la detección automatizados (p. ej., del servidor LWM2M y BSF), GBA y LWM2M se combinan ventajosamente para eliminar el coste de la precarga de ajustes y credenciales, lo que facilita los dispositivos de bajo coste. El GBA con LWM2M admite de forma segura dispositivos de bajo coste que están desatendidos o no tienen UI, donde no hay opción para la interacción del usuario (tal como introducir un PIN) y donde no hay ningún usuario que pueda darse cuenta y recuperarse de fallos de autenticación (servidor falso, cliente falso o hombre en el medio), además, el GBA funciona sin requerir ninguna clave pública o procesamiento de certificado en el dispositivo. Esto es particularmente ventajoso en dispositivos más simples, ya que estos dispositivos pueden tener un soporte mínimo de clave pública o errores de implementación al manejar certificados.

En consecuencia, el secreto compartido puede utilizarse como clave en el estándar LWM2M. Asimismo, los procedimientos estándar LWM2M pueden utilizarse para la transmisión y/o recepción de cualquier comunicación utilizada dentro del GBA.

El secreto compartido se puede usar como clave o secreto compartido dentro del protocolo DTLS (identificado en el apartado anterior "Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema"), ya sea cuando el LWM2M se utiliza junto con un protocolo DTLS o cuando el DTLS se

utiliza solo o junto con uno o más protocolos.

La comunicación segura puede ser además una comunicación de datos. La comunicación de datos puede ser una comunicación basada en SMS. Se puede utilizar un enlace de SMS. La comunicación de datos puede ser una comunicación basada en UDP.

El procedimiento puede comprender además cifrar una comunicación a través de la comunicación de datos segura. El cifrado se puede realizar mediante un estándar de cifrado avanzado. La comunicación basada en SMS puede asegurarse aún más mediante el uso de un protocolo durante la comunicación (OTA), p. ej., una estructura de paquetes segura para aplicaciones UICC. Este protocolo se define en el estándar ETSI 102.225. El protocolo OTA puede disponerse para asegurar la comunicación con la tarjeta de identificación asociada con el dispositivo.

También se ha observado que el protocolo OTA se puede utilizar ventajosamente junto con el estándar LWM2M, en el que el LWM2M se puede utilizar para gestionar parámetros, claves y elementos parecidos en el protocolo OTA.

El uso de OTA con LWM2M no es una implementación sencilla. El OTA es una solución diseñada para la seguridad de la tarjeta SIM, ya que presenta algunos desafíos técnicos reales si se usa en LWM2M. En particular, si bien existe software escrito para tarjetas SIM y servidores SIM OTA que admiten el estándar ETSI 102.225, no existe un software parecido en el espacio de gestión de dispositivos para dispositivos (y, en particular, no para clientes y servidores OMA DM). Así, los fabricantes de dispositivos M2M no tienen un código base que puedan adaptar fácilmente para su uso con estos dispositivos.

Además, el estándar ETSI 102.225 no explica cómo establecer las claves y parámetros para su uso con el estándar. Sencillamente supone que todas las claves y parámetros están precargados y son conocidos tanto por la tarjeta SIM como por el servidor OTA. Aunque esta suposición es aceptable en el espacio SIM (porque las tarjetas SIM pueden proveerse de forma segura con las claves necesarias en la etapa de fabricación y los fabricantes de SIM tienen interfaces con los operadores para comunicar las claves y parámetros necesarios), no se puede decir lo mismo sobre LWM2M, donde esa infraestructura no existe.

Así, el uso de OTA junto con LWM2M crea una combinación nueva e innovadora que produce un efecto sinérgico y proporciona muchas ventajas técnicas. Por ejemplo, es necesario asegurar el portador de SMS y hasta ahora no se ha encontrado ninguna solución. El uso de OTA permite utilizar el portador de SMS en LWM2M. Sin él, no sería posible utilizar comunicaciones basadas en SMS en LWM2M y eso limitaría la aplicabilidad del estándar LWM2M global.

En consecuencia, se pueden utilizar los procedimientos estándar LWM2M para gestionar los parámetros y/o claves utilizadas en el protocolo OTA. El procedimiento se puede utilizar además junto con LWM2M, como se describe anteriormente.

También se ha observado que el procedimiento descrito anteriormente, implementado con el GBA (o una arquitectura parecida), se puede utilizar junto con SMS de modo que se pueda emplear GBA para establecer claves en comunicaciones seguras basadas en SMS (p. ej., SMS), mientras que al mismo tiempo las comunicaciones basadas en SMS se pueden utilizar para transportar o llevar mensajes asociados con el GBA; por ejemplo, llevar mensajes con información de inserción de GBA (GPI). El uso de comunicaciones basadas en SMS junto con el GBA crea una combinación nueva e innovadora que produce un efecto sinérgico y proporciona muchas ventajas técnicas. Por ejemplo, el GBA se puede utilizar para establecer las claves compartidas necesarias para proteger los SMS y, al mismo tiempo, utilizar SMS como transporte para entregar los mensajes GBA necesarios. Además, los SMS utilizados para entregar los mensajes GBA pueden ser protegidos por integridad (y cifrados parcialmente) utilizando las claves establecidas por GBA, por lo que en ningún momento se depende de SMS no seguros. Esta combinación sinérgica permite el uso de SMS como único portador para el tráfico M2M, algo que de otro modo no sería posible, a menos que se carguen previamente las claves necesarias para asegurar el tráfico SMS, o se cambie a un protocolo diferente para negociar estas claves: ambas alternativas añadirían complejidad y coste. Así, proporcionaría una solución de muy alta seguridad para obtener claves compartidas de modo que la seguridad de las claves no se vea comprometida y, al mismo tiempo, se permite una comunicación basada en SMS en virtud del aprovisionamiento de las claves.

En consecuencia, cuando el procedimiento se implementa mediante GBA, el GBA puede utilizarse para establecer claves para la transmisión y/o entrega segura de SMS. Las comunicaciones basadas en SMS pueden utilizarse para la transmisión y/o recepción de cualquier comunicación utilizada dentro del GBA, teniendo en cuenta que estas comunicaciones pueden estar protegidas con las claves que se derivarán en GBA.

Además de lo anterior, el servidor puede comprender además un componente de autenticación de servidor. Asimismo, el cliente puede comprender además un componente de autenticación de cliente. El componente de autenticación del servidor puede realizar la autenticación del servidor con el componente de autenticación. El componente de autenticación de cliente puede realizar la autenticación del cliente con el componente de autenticación.

Además, el componente de autenticación puede ser una función de servidor de arranque (BSF), el componente de autenticación del servidor puede ser una función de aplicación de red (NAF) y el componente de autenticación del cliente puede ser un servidor GAA.

El procedimiento puede comprender además la comunicación entre el servidor y el cliente para determinar los parámetros de seguridad que se utilizarán para la comunicación segura, en el que la comunicación se realiza mediante un protocolo de gestión de dispositivos (por ejemplo, el GBA). La comunicación segura puede ser para su uso en el protocolo de gestión de dispositivos.

En una realización adicional, se proporciona un procedimiento que permite una comunicación segura para su uso en un dispositivo y/o protocolo de gestión de servicios/aplicaciones, siendo la comunicación segura entre un servidor y un cliente, estando asociado el cliente con un dispositivo, requiriendo la comunicación segura que se acuerden parámetros de seguridad entre el cliente y el servidor, comprendiendo el procedimiento comunicarse entre el servidor y el cliente para acordar los parámetros de seguridad, en el que la comunicación se realiza mediante el protocolo de gestión de dispositivos. El dispositivo puede ser un dispositivo M2M.

En una realización adicional, se proporciona un aparato, sistema, módulo o red para permitir una comunicación segura con un dispositivo, siendo dicha comunicación entre un servidor y un cliente, estando asociado el cliente con el dispositivo. Además, el aparato, sistema, módulo o red puede incluir también medios para realizar una cualquiera de las etapas o características de los procedimientos descritos anteriormente. El dispositivo puede ser un dispositivo M2M.

En una realización adicional, se proporciona un aparato, sistema, módulo o red para permitir una comunicación segura para su uso en un dispositivo y/o protocolo de gestión de servicios/aplicaciones, siendo la comunicación segura entre un servidor y un cliente, estando asociado el cliente con un dispositivo, la comunicación segura requiere que se acuerden parámetros de seguridad entre el cliente y el servidor, el procedimiento comprende la comunicación entre el servidor y el cliente para acordar los parámetros de seguridad, en el que la comunicación se realiza mediante el protocolo de gestión de dispositivos. Además, el aparato, sistema, módulo o red puede incluir también medios para realizar una cualquiera de las etapas o características de los procedimientos descritos anteriormente. El dispositivo puede ser un dispositivo M2M.

En una realización adicional, se proporciona un cliente que incluye cualquier medio, característica o funcionalidad correspondiente a los medios, características o funcionalidades relativas al cliente tal como se menciona en uno cualquiera de los procedimientos descritos anteriormente.

En una realización adicional, se proporciona un servidor que incluye cualquier medio, característica o funcionalidad correspondiente a los medios, características o funcionalidades relativas al servidor tal como se menciona mediante uno cualquiera de los procedimientos descritos anteriormente.

En una realización adicional, se proporciona un dispositivo que comprende una tarjeta y un cliente, en el que el dispositivo está dispuesto para permitir una comunicación segura, siendo la comunicación segura entre un servidor y el cliente, en el que el aprovisionamiento de la comunicación segura está basado en una asociación de seguridad entre una red y la tarjeta. El cliente puede comprender cualquier medio, característica o funcionalidad correspondiente a los medios, características o funcionalidades relativas al cliente tal como se menciona en uno cualquiera de los procedimientos descritos anteriormente. El dispositivo puede ser un dispositivo M2M.

En una realización adicional, se proporciona un servidor dispuesto para permitir la comunicación segura con un dispositivo, siendo la comunicación segura entre el servidor y un cliente asociado con el dispositivo, en el que el aprovisionamiento de la comunicación segura está basado en una asociación de seguridad entre una red y una tarjeta, estando asociada la tarjeta con el dispositivo. El servidor puede comprender cualquier medio, característica o funcionalidad correspondiente a los medios, características o funcionalidades relativas al servidor tal como se menciona en uno cualquiera de los procedimientos descritos anteriormente. El dispositivo puede ser un dispositivo M2M.

En una realización adicional, se proporciona un sistema para permitir la comunicación segura con un dispositivo, siendo dicha comunicación entre un servidor y un cliente, estando asociado el cliente con el dispositivo, en el que el aprovisionamiento de la comunicación segura está basado en una asociación de seguridad entre una red y una tarjeta, estando asociada la tarjeta con el dispositivo. El dispositivo puede ser un dispositivo M2M.

En una realización adicional, se proporciona un procedimiento que permite la comunicación segura de datos con un dispositivo, siendo la comunicación entre un servidor y un cliente asociado con el dispositivo, en el que la seguridad de la comunicación se habilita mediante un secreto de arranque. El dispositivo puede ser un dispositivo M2M. El protocolo de seguridad se puede utilizar para asegurar la comunicación de datos. El secreto de arranque se puede utilizar para obtener los elementos de seguridad utilizados en el protocolo seguro. El secreto de arranque puede ser un secreto precompartido, siendo dicho secreto proporcionado directamente al servidor y al cliente. El secreto precompartido puede proporcionarse permanentemente al servidor y al cliente (p. ej., proveer previamente al cliente y/o al servidor de dicho secreto precompartido, p. ej., en la etapa de fabricación o antes de que el cliente y/o el servidor sean utilizados en un sistema). El secreto precompartido puede ser un secreto precompartido fuerte y de alta entropía o un secreto precompartido temporal de baja entropía. El secreto de arranque puede basarse en una clave pública o en un procedimiento basado en certificados. El secreto de arranque se puede proporcionar por medio de un servidor de arranque. Los elementos de seguridad pueden ser llaves y/o disposiciones parecidas bien conocidas en la técnica.

La comunicación puede ser una comunicación basada en SMS. El protocolo de seguridad se define en ETSI TS

102.225. El procedimiento puede utilizar enlace de SMS. El dispositivo puede estar asociado además con una tarjeta, y la seguridad de la comunicación de datos puede controlarse por medio de la tarjeta. Cualquier comunicación entrante basada en SMS puede descifrarse y/o verificarse por medio de la tarjeta, y/o cualquier comunicación saliente basada en SMS puede cifrarse y/o verificarse por medio de la tarjeta.

La comunicación puede ser una comunicación basada en UDP. El protocolo de seguridad puede ser un protocolo DTLS.

La comunicación de datos segura puede proporcionarse a través de una interfaz de comunicación. La interfaz de comunicación se puede utilizar para gestionar el dispositivo o para gestionar las operaciones de arranque.

La comunicación de datos puede realizarse según el protocolo LWM2M.

En una realización adicional, se proporciona un aparato, sistema, módulo o red que permite la comunicación segura de datos con un dispositivo, siendo la comunicación entre un servidor y un cliente asociado con el dispositivo, en el que la seguridad de la comunicación se habilita mediante un secreto de arranque. El dispositivo puede ser un dispositivo M2M.

En una realización adicional, se proporciona un procedimiento para recuperar elementos de seguridad necesarios que permiten la comunicación segura de datos con un dispositivo, siendo la comunicación entre un servidor y un cliente asociado con el dispositivo, en el que los elementos de seguridad se recuperan mediante un protocolo de arranque. El dispositivo puede ser un dispositivo M2M. El protocolo de arranque puede recuperar los elementos de seguridad en una sesión segura. La sesión puede asegurarse basándose en un protocolo de seguridad. El protocolo de seguridad puede ser un protocolo DTLS. El protocolo de arranque puede estar basado en GBA. La comunicación de datos puede ser una comunicación basada en SMS. El protocolo de arranque puede ser un protocolo de arranque LWM2M. Los elementos de seguridad pueden ser llaves y/o disposiciones parecidas bien conocidas en la técnica.

En una realización adicional, se proporciona un aparato, sistema, módulo o red que permite la comunicación segura de datos con un dispositivo, siendo la comunicación entre un servidor y un cliente asociado con el dispositivo, en el que los elementos de seguridad se recuperan mediante un protocolo de arranque. El dispositivo puede ser un dispositivo M2M.

La comunicación segura puede tener el propósito de gestionar el dispositivo y/o el cliente y/o los servicios (p. ej., proporcionados por el dispositivo) por parte del servidor. Tanto el dispositivo como el servidor pueden ser máquinas (es decir, que no requieren ninguna intervención humana para funcionar). Cuando el dispositivo es una máquina, se puede utilizar el servidor para gestionarlo. Nuevamente, la gestión se puede realizar sin ninguna intervención humana (p. ej., automáticamente).

Como se analiza anteriormente, la solución podría utilizarse junto con el protocolo LWM2M, pero la solución podría extenderse a otros protocolos de gestión de dispositivos o a otros servicios M2M (p. ej., asegurar la entrega de SMS binarios). En particular, y como se analiza anteriormente, el uso de la solución junto con un protocolo específico de M2M, tal como LWM2M, permite que la solución sea muy eficaz cuando se utiliza con dispositivos M2M y, en particular, cuando se utiliza para gestionar el dispositivo y/o servicios proporcionados por (o por medio de) el dispositivo. En otras palabras, todas las ventajas mencionadas anteriormente se mejoran y optimizan aún más cuando la solución se utiliza junto con un protocolo específico de M2M.

Además, también se proporciona cualquier aspecto o combinación de aspectos según una cualquiera de las reivindicaciones.

También se proporciona cualquier combinación de las características descritas en relación con cualquiera de los aspectos, incluso si no se divulga explícitamente.

En referencia a la figura 2, se muestra una arquitectura (100) ejemplar que puede implementarse, en particular cuando se utiliza GBA. Un dispositivo 110 (en el ejemplo, un dispositivo M2M y/o un equipo de usuario) está asociado con una tarjeta 112 (en el ejemplo, una UICC) y un cliente 116 (en el ejemplo, un cliente de gestión de dispositivos (DM). Obsérvese que este cliente también podría ser un cliente LWM2M, concretamente, un cliente que puede gestionar el dispositivo en sí y los servicios/aplicaciones proporcionadas por el dispositivo, p. ej., control de activos). El dispositivo 110 también está asociado con un componente 114 de autenticación de dispositivo (en el ejemplo, un servidor GAA). Además, se proporciona un servidor 120 (en el ejemplo, un servidor DM), el servidor asociado con un componente 122 de autenticación de servidor (en el ejemplo, una función de aplicación de red (NAF)). Además, se proporciona un componente 130 de autenticación (en el ejemplo, una función de servidor de arranque (BSF)) y un registro 140 (en el ejemplo, un HLR o HSS). Asimismo, se proporcionan cuatro interfaces diferentes para la comunicación entre los diversos componentes, en particular la interfaz Ua 150 entre el dispositivo 110 y el servidor 120, la interfaz Ub 160 entre el dispositivo 110 y el componente 130 de autenticación, la interfaz Zn 170 entre el componente 130 de autenticación y el servidor 120, y la interfaz Zh/Zh' entre el componente 130 de autenticación y el registro 140.

En particular, en referencia a GBA, el documento TS 33.220 define los siguientes componentes e interfaces, que se muestran en la figura 2. La NAF, la "función de aplicación de red", es un componente del lado del servidor de una aplicación que puede asegurarse mediante GBA. En una realización preferida, la NAF puede ser un componente de

software dentro de un servidor de gestión de dispositivos (DM).

Algunos aspectos de BSF, HLR/HSS, UE, Ua, Ub, Zh/Zh' y Zn se proporcionan en el apartado anterior "Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema".

Tras la autenticación satisfactoria del dispositivo 110, la BSF 130 deriva el secreto compartido Ks NAF, que es recuperado por la NAF. En una realización preferida, lo más probable es que la BSF 130 esté en un servidor separado del HLR/HSS 140, pero dentro de un grupo de plataformas M2M.

El HLR/HSS puede ser "compatible con GBA" (para que almacene detalles del abono de un usuario de GBA) o puede ser un componente heredado. En una realización preferida, el HLR/HSS sería el HLR o HSS de un operador móvil M2M (es decir, uno dedicado específicamente a prestar servicio a conexiones M2M).

El UE 110 es, en la solución propuesta, un dispositivo M2M.

En una realización preferida, la Ua es la interfaz entre un cliente 116 de gestión de dispositivos y un servidor 120 de gestión de dispositivos.

En una realización preferida, la Ub sería la interfaz entre el componente 114 "servidor GAA" del dispositivo y la BSF 130.

En una realización preferida, se utiliza la interfaz Zn.

En la solución propuesta, esta interfaz está entre el servidor 120 de gestión de dispositivos y la BSF 130. La versión WS de la interfaz permitiría la colocación de un servidor DM en múltiples ubicaciones (no solo en el grupo de plataformas/operadores M2M) y permitiría NAF futuras en múltiples ubicaciones.

En referencia a la figura 3, a continuación, se describe el procedimiento para establecer la comunicación segura según la presente invención, en particular cuando se utiliza GBA.

En 205, el UE 110 se pone en contacto a través de la interfaz Ua con la NAF 122 (en la realización descrita, el cliente 116 de gestión de dispositivos se pone en contacto con el servidor 122 de gestión de dispositivos) y detecta que la NAF requiere que adquiera un secreto compartido usando GBA. Esto podría deberse a que no existe ningún secreto, o que el secreto existente haya caducado o que la NAF lo considere inválido.

La interfaz exacta y el procedimiento de comunicación pueden ser específicos de la aplicación en cuestión. A continuación, se analiza una posible interfaz y procedimiento de comunicación para M2M OMA de baja complejidad.

A través de la interfaz UE interna desde el cliente DM al servidor GAA: en 210, el cliente 116 DM solicita al servidor 114 GAA obtener un secreto compartido. Presenta un identificador para la NAF correspondiente (NAF_Id).

A través de la interfaz Ub: en 215, el UE 110 se pone en contacto con la BSF (el servidor 114 GAA se pone en contacto con la BSF 130). Esta puede ser una petición HTTP GET básica. El UE presenta un "IMPI" (equivalente a un IMSI) o un "TMPI" (equivalente a un TMSI) por motivos de anonimato, si hay alguno disponible.

A través de la interfaz Zh o Zh': en 220, la BSF 130 solicita un vector de autenticación del HLR/HSS 140. En 225, el HLR/HSS 140 devuelve un vector nuevo, que consiste en RAND, AUTN, XRES, CK e IK, por ejemplo.

La BSF 130 genera un identificador de transacción (B-TID) y pasa (230) el B-TID junto con el RAND y el AUTN de regreso al UE 110. También puede indicar la duración del B-TID y la clave asociada.

A través de la interfaz UE interna desde el servidor GAA a la UICC: en 235, el servidor 114 GAA reenvía el RAND y el AUTN a la UICC 112 que valida el AUTN. Si el AUTN es válido, entonces se autentica la BSF 130. En 240, la UICC 112 devuelve un RES, CK e IK al servidor 114 GAA.

En 245, el UE 110 (servidor 114 GAA) se pone en contacto nuevamente con la BSF 130, utilizando el RES resultante en la autenticación implícita HTTP (que se identifica en el apartado anterior "Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema").

La BSF 130 verifica la autenticación implícita HTTP utilizando XRES. Si coincide, entonces el UE 110 se ha autenticado satisfactoriamente. La BSF 130 almacena la tupla <IMPI, B-TID, RAND, CK, IK> y le dice en 250 al UE 110 que la autenticación fue satisfactoria. La UE 110 almacena <B-TID, RAND, CK, IK>.

A través de la interfaz interna del UE 110 desde el cliente 116 DM al servidor 114 GAA: el UE 110 (servidor 114 GAA) deriva una Ks_NAF secreta utilizando el CK, IK, RAND, IMPI y NAF_Id. En 255, pasa la Ks_NAF y el B-TID de vuelta al cliente 116 DM.

A través de la interfaz Ua nuevamente: en 260, el UE 110 (cliente 116 DM) se pone en contacto con la NAF (servidor 122 DM) y presenta el B-TID según se ha recuperado anteriormente.

A través de la interfaz Zn: en 265, la NAF 122 se pone en contacto con la BSF 130 y presenta el BTID. La BSF 130

autentica la NAF, deriva la Ks_NAF correspondiente y en 270 la devuelve a la NAF, junto con un indicador de la duración de la clave.

El UE 110 (cliente 116 DM) y la NAF (servidor 122 DM) ahora comparten la Ks_NAF. Pueden utilizarla directamente o derivar sus propias claves de sesión para una mayor comunicación.

Nuevamente, la interfaz exacta y el procedimiento de comunicación pueden ser específicos de la aplicación en cuestión. A continuación, se analiza una posible interfaz y procedimiento de comunicación para M2M OMA de baja complejidad.

Como se analiza anteriormente, la solución podría utilizarse junto con el estándar LWM2M. Este estándar puede verse como un sucesor de los estándares de gestión de dispositivos OMA existentes (OMA DM 1.0 a 1.3), pero altamente optimizado para dispositivos de tipo máquina de gama baja y con un ámbito de gestión extendido más allá del propio dispositivo, que incluye la gestión de servicios proporcionados por el dispositivo M2M tal como el control de activos. Esto contrasta, por ejemplo, con el OMA DM 2.0, que es el sucesor de dispositivos de consumo como teléfonos inteligentes, tabletas, etc. Otros estándares de gestión de dispositivos ampliamente utilizados incluyen el TR-069, que fue desarrollado por Broadband Forum para gestionar equipos en las instalaciones del cliente (en particular módems DSL).

El flujo ejemplar descrito en referencia a la figura 3 es muy genérico y puede usarse con muchos tipos diferentes de protocolos de gestión de dispositivos (u otros protocolos de aplicación). Como se puede observar, muchos detalles de la interfaz Ua están fuera del ámbito de 3GPP y se dejan para que otros estándares los completen (o se dejan a implementaciones propias). Sin embargo, la integración con el estándar LWM2M es posible, como se describe en estos ejemplos.

Según la especificación (véase anteriormente), la seguridad para OMA LWM2M se basa en DTLS v1.2 (véase más arriba) y CoAP (véase más arriba). Tanto el cliente como el servidor deben admitir DTLS de clave precompartida (p. ej., véase la sección 7.1.1, página 41), mientras que el soporte para la autenticación basada en certificados es solo opcional. Esto significa que una clave derivada del GBA (Ks_NAF) podría utilizarse como una clave precompartida DTLS y funcionaría con cualquier par de cliente DM/servidor DM.

Se hace referencia al planteamiento general para TLS de clave precompartida en el apartado anterior "Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema". Los protocolos GBA y TLS-PSK funcionan bien juntos. En 205 descrito anteriormente, el mensaje "hola del servidor" contiene un campo donde el servidor puede indicar que admite el arranque GBA y, en respuesta, el cliente ya puede proporcionar un identificador (B-TID) de una clave (260) de arranque. O si el cliente aún no tiene una clave de arranque, le pide al servidor GAA que obtenga una, antes de reanudar el "hola del cliente" y el "hola del servidor" en 260. El uso de la Ks_NAF para derivar las claves de sesión se especifica completamente dentro del protocolo TLS-PSK. La especificación 3GPP supone HTTP/TLS, pero el planteamiento básico es el mismo para CoAP/DTLS.

Para mejorar la coherencia con el perfil OMA del GBA, es posible que la especificación LWM2M deba definir un "identificador de protocolo" para la clave precompartida DTLS y que OMNA la registre (véase la sección 5.2.1 del perfil OMA GBA, versión aprobada 1.1 - 31 julio de 2012 que se encuentra en http://technical.openmobilealliance.org/Technical/release_program/sec_of_archive.aspx).

Aparte de los aspectos GBA, el dispositivo M2M puede configurarse para admitir la seguridad de OMA LWM2M, a la que se hace referencia en el apartado anterior "Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema".

Aspectos adicionales

1. Desarrollo de dispositivos para GBA

Como se puede observar en la figura 2 y la figura 3, el dispositivo M2M puede contener varios componentes internos. Debería admitir un cliente DM que sea "compatible con GBA", así como un componente del "servidor GAA".

El componente del servidor GAA debe admitir interfaces internas para el cliente DM y la tarjeta SIM (UICC), así como la interfaz Ub externa para la BSF. La interfaz con la UICC puede ser particularmente difícil, ya que es posible que el dispositivo M2M no exponga una API existente para que el software del dispositivo pueda enviar comandos a la UICC. Una posibilidad (que puede utilizarse) es que el módem exponga comandos AT. Sin embargo, es posible que esto no sea a un nivel suficientemente bajo (AT+CSIM permite que las APDU sin formato se comuniquen con la UICC) en todos los casos. Además, puede haber problemas de seguridad: si bien el servidor GAA debe poder interactuar con la UICC, las aplicaciones generales instaladas en el dispositivo no deberían poder utilizar esta interfaz, ya que eso podría permitir que partes externas se hagan pasar por el dispositivo (y generar fraude en la red celular). Por lo tanto, la API de la tarjeta SIM debe ser privilegiada, así como tener un nivel suficientemente bajo para ser utilizable.

2. Tunelización Ub o inserción de GBA

La interfaz de la BSF se basa en HTTP y autenticación implícita HTTP. Una alternativa puede ser "tunelizar" la interfaz

Ub dentro de la interfaz Ua, de modo que el dispositivo solo necesite admitir el protocolo CoAP (no también HTTP).

Una alternativa relacionada es utilizar la variante "inserción" de GBA y llevar mensajes de inserción (interfaz Upa) dentro de la interfaz Ua. Ambos requerirían identificar los comandos y parámetros adecuados en la interfaz Ua (es decir, el protocolo de gestión de dispositivos pertinente) para llevar el túnel o los mensajes de inserción. Las interfaces y el flujo de mensajes para la inserción de GBA se esbozan a continuación (véase también el 3GPP TS 33.223, titulado "3G Security; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function", actualmente se puede recuperar en http://www.3gpp.org/ftp/Specs/html-info/33223.htm).

En referencia a la figura 4, a continuación, se muestra un ejemplo de procesamiento y flujo de mensajes para inserción de GBA:

1. Una NAF establece una NAF SA compartida con un UE que está registrado para los servicios de inserción. Conoce la identidad del abonado.

2. La NAF-inserción genera la petición GPI (información de inserción de GBA) y envía la petición GPI a la BSF.

3. Al recibir la petición de la NAF, la BSF comprueba que la NAF esté autorizada y resuelve el identificador de abonado solicitado en un identificador privado (p. ej., IMSI).

4. La BSF obtiene un nuevo AV (vector de autenticación) y GUSS (ajustes de seguridad del usuario GBA) de abonado desde el HSS.

5. El HSS envía el AV y el GUSS a la BSF.

6. Cuando la BSF recibe la respuesta AV del HSS, genera las claves NAF basadas en el NAF_Id solicitado y crea la respuesta GPI pertinente.

7. La BSF envía la respuesta GPI a la NAF.

8. La NAF almacena la información recibida junto con otra información del usuario en una NAF SA.

9. Luego, la NAF reenvía el GPI al UE a través de Upa utilizando el mecanismo de transporte seleccionado y la dirección de transporte dada.

10. Cuando el UE recibe el mensaje que contiene el GPI, procesa el GPI como si fuera para el GBA normal y almacena las NAF SA correspondientes.

La UE y la NAF ahora están listas para utilizar la NAF SA establecida.

El TR33.223 especifica que la Upa es una nueva interfaz separada de Ua: "se introduce un nuevo punto de referencia Upa entre la NAF y el UE" (sección 4.2.1). Como tal, la interfaz Ua no debe saber si se utiliza GBA o inserción de GBA.

3. Aprovisionamiento de la dirección de la BSF y la NAF

La dirección de la BSF (http URL) puede estar precargada cuando se fabrica el dispositivo. Podría gestionarse mediante el propio dispositivo, lo que parecería crear el problema del "huevo y la gallina", pero el servidor DM podría, por ejemplo, proporcionar una dirección para una BSF aceptable en el hola del servidor. O el operador de telefonía móvil M2M podría encaminar el tráfico http a una dirección BSF por defecto. De forma similar, es posible que sea necesario precargar la ubicación del servidor DM preferido, o el operador de telefonía móvil M2M podría encaminar el tráfico CoAP a una dirección de servidor DM por defecto.

4. Tipos de GBA (GBA-ME, GBA-U, GBA-SIM, etc.)

Se hace referencia a varias versiones diferentes del GBA en el apartado "Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema". El GBA-U tiene ventajas de seguridad, pero también ventajas logísticas: permite una duración más larga del B-TID ya que la clave derivada se almacena de forma más segura. Permite la retención segura de Ks durante los ciclos de apagado, por ejemplo. El GBA-U requiere apoyo específico de la UICC, por lo que tendría un (modesto) incremento en el coste. Dado que los dispositivos M2M típicamente están provistos en cualquier caso de una UICC nueva en el momento de la fabricación, se trata de un coste de software/desarrollo en lugar de un coste de hardware. Asimismo, en un modelo con una UICC personalizada, esto puede permitir una solución que utilice comandos AT restringidos para el módem, en lugar de AT+CSIM completo.

5. Ubicación de la NAF (servidor DM) y tipo de interfaz Zn

El ejemplo de arquitectura permite que existan varios servidores DM en diferentes ubicaciones: podrían formar parte de un grupo de plataformas M2M (p. ej., un operador móvil M2M), o alojados en otro lugar por un operador de red/proveedor de servicios, o quizás por un cliente de dicho operador/proveedor. Es posible que la BSF deba estar ubicada dentro de una zona desmilitarizada (DMZ) con cortafuegos, o tal vez conectada por medio de un proxy http en la DMZ (lo que permite el acceso al servicio web http externo desde las NAF), y luego ejecutaría la interfaz del

Diámetro al HLR/HSS. Puede que no sea deseable exponer una interfaz http directamente en el servidor que admite el HLR, o hacer un túnel con Diámetro a través de cortafuegos. Sin embargo, si el servidor DM forma en sí mismo parte del grupo de plataformas M2M, entonces esto puede ser un exceso de ingeniería. Posiblemente entonces resulte aceptable una solución de Diámetro para la interfaz Zn.

6. Uso de la interfaz Zh o Zh'

Idealmente, el HLR se puede actualizar a un HSS completo con soporte para el punto de referencia Zh. Sin embargo, si el HLR/HSS solo admite Zh', entonces la BSF tendrá que ser más complicada y tomará algunas de las funciones de gestión de abonos (perfiles, duración, políticas de seguridad) típicamente asociadas con el HSS.

7. Desarrollo del componente NAF

Si bien la funcionalidad NAF parece bastante sencilla, será necesario desarrollarla para cada servidor DM utilizado y para cada aplicación adicional que utilice GBA.

Las claves GBA podrían utilizarse para proteger SMS (p. ej., cifrar/proteger la integridad de SMS usando una interfaz de paquetes segura, p. ej., como ETSI TS 102.225 que se utiliza para SIM OTA). Es probable que este canal de SMS sea más eficaz que DTLS.

Además, independientemente del GBA, un protocolo de SMS seguro podría vincularse a un protocolo de gestión de dispositivos y/o servicios, concretamente: utilizando un protocolo de SMS seguro (p. ej., diseñado originalmente para SIM OTA (102 225)), pero ahora adaptado para comunicaciones LWM2M, combinado con el uso del protocolo LWM2M para definir (y gestionar) los parámetros necesarios para el protocolo SMS seguro (es decir, los Klc, KID, SPI, TAR y claves pertinentes).

El GBA podría utilizarse para derivar las claves de forma segura.

En los párrafos siguientes se describen aspectos adicionales y características ventajosas o preferibles.

El LWM2M necesita una solución de seguridad para el portador de SMS. Sin una solución, los SMS no podrán utilizarse como portadores, lo que limitará gravemente el alcance de LWM2M. Una solución a este problema es utilizar la seguridad SIM OTA (p. ej., véase TS 102 225).

El TS 102.225 se basa en que las claves y los parámetros ya están acordados entre el cliente y el servidor. Sin embargo, es difícil precargarlos en los dispositivos cliente LWM2M y asegurar que se envíen a los servidores, porque no existe una infraestructura actual para hacerlo. No tendría sentido entregar las claves y parámetros a través de SMS no seguros.

Existen diversas soluciones propuestas para entregar estas claves y parámetros de forma segura.

En una primera solución, se proporciona conmutación de portador a UDP/Coap y ejecución de DTLS. La sesión DTLS se puede utilizar para asegurar el protocolo de arranque LWM2M. El arranque LWM2M se puede utilizar para establecer las claves y los parámetros del TS 102.225 de forma segura. Obsérvese que los recursos/objetos gestionados deben definirse para permitir que el servidor de arranque los actualice; el formato de estos recursos se especifica en los párrafos numerados a continuación.

En una segunda solución, se prevé basarse en una tarjeta SIM (UICC) que ya se ha provisto de claves y parámetros, y utilizar esta tarjeta para terminar la seguridad TS 102 225. Obsérvese que, puesto que esta solución proporciona un canal seguro, se puede utilizar el mismo canal para entregar otras claves y parámetros.

En una tercera solución, se proporciona el uso de GBA para establecer las claves y los parámetros. Esto funciona porque el GPI (información de inserción de GBA) se puede entregar a través de SMS no seguros. Por lo tanto, no es necesario tener una clave inicial para proteger el SMS. (Obsérvese que la entrega de parámetros como Kic, KID, sPI y TAR no es obvia, sino que estos son solo 6 bytes y existen campos en el GPI, p. ej., App_Lbl, NAF Id, P-TID que podrían utilizarse para llevar esta información.)

Se proporcionan más detalles en los párrafos numerados a continuación.

Se hace referencia a la seguridad del canal UDP para [COAP] en el apartado anterior "Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema".

Dado que el protocolo LWM2M utiliza DTLS para fines de autenticación, integridad de datos y confidencialidad, el cliente LWM2M y el servidor LWM2M DEBERÍAN mantener una sesión DTLS cuando se utiliza durante el período más largo que se pueda lograr de forma segura sin correr el riesgo de comprometer las claves y los contadores de la sesión. Si una sesión persiste durante los ciclos de suspensión, DEBERÍA utilizarse un almacenamiento cifrado y protegido por integridad para las claves y los contadores de la sesión.

Obsérvese que la relación cliente-servidor de DTLS (es decir, quién inició el establecimiento de la comunicación) es

independiente de la relación cliente-servidor de LWM2M.

Teniendo en cuenta que cualquier dispositivo con un cliente LWM2M puede gestionarse mediante cualquier servidor LWM2M y servidor de arranque LWM2M, la elección de conjuntos de cifrados no se limita a la lista definida en la sección 9 de [CoAP]. Debido a la naturaleza confidencial de la información de arranque, se debe tener especial cuidado en asegurar la protección de esos datos, incluidas las restricciones y dependencias dentro de una relación servidor de arranque/cliente LWM2M según el modo de seguridad adoptado.

Con respecto al arranque desde una tarjeta inteligente, se debe tener el mismo cuidado y se DEBERÍA establecer un canal seguro entre la tarjeta inteligente y el dispositivo LWM2M como se describe en el apéndice H de OMA LWM2M en referencia al protocolo de canal seguro de GlobalPlatform 03 (SCP 03) enmienda D v1.1 de septiembre de 2009.

El material para claves utilizado para asegurar el intercambio de información mediante una sesión DTLS se puede obtener utilizando uno de los modos de arranque a los que se hace referencia en el apartado anterior "Detalles de los estándares y tecnologías 3GPP utilizados para implementar aspectos del procedimiento y sistema".

Los recursos (es decir, "modo de seguridad", "clave pública o identidad", "clave pública o identidad" y "clave secreta") en el objeto de seguridad LWM2M que están asociados con el material para claves se utilizan para proporcionar seguridad del canal UDP en las interfaces de "Registro de dispositivos", "gestión de dispositivos y habilitación de servicios" y "presentación de informes de información" si la instancia del objeto de seguridad LWM2M está relacionada con un servidor LWM2M, o para proporcionar seguridad de canal en la interfaz de arranque si la instancia del objeto de Seguridad LWM2M está relacionada con un servidor arranque LWM2M.

Los clientes LWM2M DEBEN proveerse directamente de un servidor LWM2M de destino (modo de arranque de configuración previa del fabricante) para su uso o bien proveerse de un servidor de arranque LWM2M para un arranque seguro. Cualquier cliente LWM2M que admita el modo de arranque iniciado por el cliente o el servidor DEBE admitir por lo menos uno de los procedimientos seguros siguientes:

1) Arranque con un secreto precompartido fuerte (alta entropía), como se describe en la sección 7.1 de OMA LWM2M. Los conjuntos de cifrado definidos en esta sección NO DEBEN usarse únicamente con un secreto precompartido de baja entropía.

2) Arranque con un secreto precompartido temporal y de baja entropía (tal como un PIN, una contraseña y un número de serie privado) mediante el conjunto de cifrado TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256, como se define en RFC5489.

3) El arranque con una clave pública o un procedimiento basado en certificado (como se describe en las secciones 7.1.2 y 7.1.3 de OMA LWM2M). El cliente LWM2M DEBE utilizar un par de claves único, uno que sea exclusivo para cada cliente LWM2M.

Para una interoperabilidad total, un servidor de arranque LWM2M DEBE admitir todos estos procedimientos.

NOTA: el servidor de arranque LWM2M también puede utilizar los procedimientos de seguridad anteriores para proveer el Klc y KID en la seguridad del canal SMS (véase, a continuación, la seguridad del canal SMS).

Seguridad del canal SMS

Modo de estructura de paquetes seguros SMS

La estructura de paquetes seguros está basada en [3GPP TS 31 115]/[ETSI TS 102 225]], que define paquetes seguros para diferentes mecanismos de transporte. La solución se diseñó originalmente para asegurar estructuras de paquetes en aplicaciones basadas en UICC; sin embargo, en LWM2M es adecuada para asegurar la carga útil de SMS intercambiada entre el cliente y el servidor.

El modo de estructura de paquetes seguros SMS especificado en esta sección DEBE admitirse cuando se utiliza el enlace de SMS.

Un cliente LWM2M que utiliza el enlace de SMS DEBE proveerse directamente para su uso de un servidor LWM2M de destino (modo de arranque de configuración previa del fabricante o aprovisionamiento de tarjeta inteligente) o bien arrancar por medio del enlace UDP.

El punto final para el canal de SMS (entrega de SMS terminados en dispositivos móviles y envío de SMS originados en dispositivos móviles) DEBERÍA estar en la tarjeta inteligente o en el dispositivo. Cuando el dispositivo cliente LWM2M no admite una tarjeta inteligente, el punto final está en el dispositivo cliente LWM2M.

Un cliente, servidor o servidor de arranque LWM2M que admita el enlace de SMS DEBERÍA descartar los mensajes SMS que no estén correctamente protegidos utilizando los parámetros previstos almacenados en el recurso "parámetros de clave de enlace de SMS" y las claves previstas almacenadas en el recurso "claves secretas de enlace de SMS", y NO responderá con un mensaje de error seguro utilizando los parámetros y claves correctos.

Punto final del dispositivo

Si el punto final del canal SMS está en el dispositivo, se DEBERÁN aplicar los ajustes siguientes:

SMS de clase 1 según se especifica en [3GPP TS 23.038]

TP-PID de 111101 (descarga de datos ME) según se especifica en [3GPP TS 23.040]

TP-OA: la TP-OA (dirección de origen según se define en [3GPP 23.040] de un paquete de comando entrante (p. ej., petición CoAP) DEBE reutilizarse como la TP-DA del paquete saliente (p. ej., respuesta CoAP)

Punto final de tarjeta inteligente

Si el punto final del canal SMS está en la tarjeta inteligente, SE DEBERÁN aplicar los ajustes siguientes:

SMS de clase 2 según se especifica en [3GPP TS 23.038]. El encabezado de SMS [3GPP TS 23.040] DEBE definirse de la siguiente manera:

- TP-PID: 111111 (descarga de datos USIM) según se especifica en [3GPP TS 23.040]
- TP-OA: la TP-OA (dirección de origen según se define en [3GPP 23.040] de un paquete de comando entrante (p. ej., petición CoAP) DEBE reutilizarse como la TP-DA del paquete saliente (p. ej., respuesta CoAP)

Mecanismos del modo de paquete seguro SMS

1. Transferencia segura de SMS a UICC

Un paquete seguro SMS que encapsula una petición CoAP recibida por el dispositivo LWM2M DEBE, según [ETSI TS 102 225]/[3GPP TS 31.115], dirigirse a la aplicación UICC LWM2M en la tarjeta inteligente donde se descifrará y se agregará si es necesario y se comprobará su integridad.

Si el descifrado y la verificación de integridad son satisfactorios, el mensaje contenido en el SMS DEBE proporcionarse al cliente LWM2M.

Si falla el descifrado o la verificación de integridad, se DEBE descartar el SMS.

El mecanismo para proporcionar la petición CoAP descifrada al cliente LWM2M se basa en los comandos básicos GET DATA de [GP SCP03]. Estos datos DEBEN seguir el formato que se muestra a continuación.

data rcv::= <address> <coap msg>

address ::= TP OA ; dirección de origen

coap msg::= COAP TAG <coap request length> <coap request>

coap request length::= 16BITS VALUE

coap request::= CoAP message payload

NOTA: en la versión actual de LWM2M, la forma en que se activa la aplicación cliente LWM2M para recuperar el mensaje disponible de la tarjeta inteligente queda a discreción del dispositivo: es decir, un dispositivo LWM2M de clase media que implementa el conjunto de herramientas [ETSI TS 102 223] con clase "e" y soporte "k" podría activarse automáticamente mediante los mecanismos del conjunto de herramientas, mientras que un dispositivo LWM2M más sencillo podría basarse en mecanismos de sondeo en la tarjeta inteligente para extraer datos cuando estén disponibles.

2. Transferencia de SMS segura al servidor LWM2M

Para enviar un mensaje CoAP al servidor LWM2M, el cliente LWM2M prepara datos que contienen el TP-DA correcto para usar, concatenado con el mensaje CoAP y DEBE proporcionar esos datos a la aplicación UICC LWM2M cuando utiliza el comando STORE-DATA [GP SCP03].

Según [ETSI TS 102 225]/[3GPP TS 31.115] la tarjeta inteligente será la encargada de preparar (cifrado/concatenación) el mensaje CoAP antes de enviarlo como un paquete seguro de SMS (comando SEND_SMS [ETSI TS 102 223]).

El paquete seguro de SMS DEBE tener el formato de datos seguro especificado en la sección 7.3.1.2.

El canal seguro según se especifica en el anexo H DEBERÍA utilizarse para proporcionar los datos preparados en la tarjeta inteligente.

La seguridad del canal SMS la proporciona la estructura de paquetes seguros [ETSI TS 102 225] y [SCP080] que define paquetes seguros para diferentes mecanismos de transporte.

La solución fue diseñada originalmente para estructuras de paquetes seguras en aplicaciones basadas en UICC; sin embargo, en LWM2M es adecuada para asegurar el canal SMS entre el cliente y el servidor.

La seguridad del canal SMS especificada en esta sección DEBE aplicarse cuando se utiliza el enlace de SMS.

Cuando el dispositivo LWM2M admite una tarjeta inteligente, la seguridad DEBE finalizar en la tarjeta inteligente. El cliente LWM2M DEBE pasar mensajes SMS a la tarjeta inteligente para el cifrado y protección de la integridad antes de enviarlos, y DEBERÍA pasar mensajes SMS cifrados recibidos desde el servidor LWM2M a la tarjeta inteligente para el descifrado y comprobación de la integridad.

Un cliente LWM2M que admita el enlace de SMS DEBERÍA admitir la estructura de paquetes seguros como se define en [ETSI TS 102 225] y [SCP080]. El cliente LWM2M DEBERÍA compartir las claves pertinentes, identificadas por Klc y KID, con un servidor arranque LWM2M durante el arranque, o con un servidor LWM2M en caso contrario.

Un servidor de arranque LWM2M que admite el enlace de SMS DEBERÍA admitir la estructura de paquetes seguros como se define en [ETSI TS 102 225] y [SCP080].

Un servidor LWM2M que admite el enlace de SMS DEBERÍA admitir la estructura de paquetes seguros como se define en [ETSI TS 102 225] y [SCP080].

En el modo de estructura de paquetes seguros de SMS, un mensaje CoAP como se define en [CoAP] DEBE encapsularse en paquetes seguros [3GPP 31.115], al implementar, para SMS punto a punto (SMS PP), la especificación general [ETSI 102 225] para aplicaciones basadas en UICC.

Los párrafos siguientes son aplicables al cliente LWM2M, al servidor de arranque LWM2M y al servidor LWM2M:

- El comando "paquete de comando" especificado en [3GPP 31.115]/[ETSI TS 102 225] DEBE utilizarse tanto para el mensaje de petición como para el de respuesta CoAP.
- La estructura del paquete de comando contenido en el mensaje corto DEBE seguir la especificación [3GPP 31.115].
- NO SE DEBE basarse en un DES único.
- DEBE utilizarse AES o Triple DES con tres claves diferentes.
- Preferiblemente, se debe utilizar AES. Cuando se utiliza AES, se debería utilizar con el modo CBC para el cifrado (véase la codificación de Klc en [ETSI TS 102 225] sección 5.1.2) y en modo CMAC para la integridad (véase la codificación de KID en [ETSI TS 102 225] sección 5.1.3).
- SPI DEBERÍA establecerse de la siguiente manera (véase la codificación de SPI en [ETSI TS 102 225] sección 5.1.1):
  - suma de comprobación criptográfica
  - cifrado
    - La suma de comprobación criptográfica y de cifrado DEBE utilizar AES o Triple DES
    - NO SE DEBE utilizar un DES único
    - DEBERÍA utilizarse AES
    - Cuando se utiliza Triple DES, DEBE utilizarse en modo CBC externo y DEBEN utilizarse 3 claves diferentes
    - Cuando se utiliza AES, DEBE utilizarse con el modo CBC para el cifrado (véase la codificación de Klc en [ETSI TS 102 225] sección 5.1.2) y en modo CMAC para la integridad (véase la codificación de KID en [ETSI TS 102 225] sección 5.1.3
  - procesar si y solo si el valor del contador es mayor que el valor en el RE
- Preferiblemente, TAR (véase la codificación de TAR en [ETSI TS 101 220], sección 6) DEBERÍA establecerse en un valor en el intervalo BF FF 00 - BF FF FF.

NOTA: se solicitará un TAR para la seguridad de SMS LWM2M a ETSI SCP y el intervalo anterior es aplicable solo hasta que se haya asignado el TAR.

- Datos seguros: contienen el mensaje de aplicación seguro que DEBE codificarse como BER-TLV; la etiqueta (TBD: por ejemplo, 0x05) indicará el tipo (p. ej., tipo CoAP) de ese mensaje.

Habrá dos TAR diferentes para finalizar la seguridad en la tarjeta inteligente o en el dispositivo.

Las claves de cifrado e integridad y los valores de contador asociados DEBERÍAN mantenerse en una tarjeta inteligente o en otro entorno de almacenamiento seguro a prueba de manipulaciones (p. ej., un elemento seguro integrado). El cliente DEBERÍA pasar el MT SMS a la tarjeta inteligente/SE para el descifrado y comprobación de la integridad, y DEBERÍA pasar el MO SMS a la tarjeta inteligente/SE para el cifrado y la protección de la integridad antes de enviarlo.

Si las claves y los valores de contador asociados no se almacenan de la forma recomendada anteriormente, DEBERÍAN tratarse como claves de sesión con una durabilidad no mayor que la durabilidad del registro. El cliente LWM2M DEBERÍA adquirir nuevo material para claves, descartarlo en cada operación de 'Registro" o "Actualización", cargar material para claves nuevo utilizando uno de los mecanismos que se describen a continuación y restablecer los contadores.

- Prearranque por medio del mecanismo de inserción de GBA, como se describe en la sección 9.3.1.3 de [OMA DM v2.0]. La inserción de GBA utiliza una UICC para generar el llamado secreto compartido Ks_(ext/int)_NAF tanto en la red como en el dispositivo. A partir de esta clave maestra Ks_(ext/int)_NAF, se generan dos secretos de sesión: el DMBEK y el DMBIK. El valor de Klc (clave de cifrado para SMS) DEBERÍA establecerse truncando el DMBEK a la longitud de clave pertinente (tomando los bits 0 a 127 para AES-128, o los bits 0 a 167 bits para 3DES), y el valor de KID (clave de integridad para SMS) DEBERÍA establecerse de forma parecida truncando el DMBIK a la longitud de clave pertinente (bits 0 a 127 para AES-128, o bits 0 a 167 para 3DES). La información de inserción de GBA DEBERÍA entregarse al cliente LWM2M mediante un SMS de clase 1 según se especifica en [3GPP TS 23.038] con un TP-PID de 111101 (descarga de datos ME) según se especifica en [3GPP TS 23.040].

- Prearranque desde la tarjeta inteligente mediante uno de los procedimientos siguientes:

  - Utilizando el mecanismo de inserción de GBA descrito anteriormente, específicamente con el GBA-U, y con la tarjeta inteligente generar el DMBIK y DMBEK a partir de Ks_int_NAF.

  - Utilizando la gestión de archivos remota (RFM) o la gestión de aplicaciones remota (RAM) según se especifica en [ETSI TS 102.226]. El servidor LWM2M DEBERÍA generar nuevos datos clave aleatorios de longitud adecuada para Klc y KID y asegurar que se entregan a la tarjeta inteligente mediante un SMS de clase 2 según se especifica en [3GPP TS 23.038] con un TP-PID de 111111 (descarga de datos USIM) según se especifica en [3GPP TS 23.040], protegido mediante las claves de seguridad OTA pertinentes para RFM o RAM.

La tarjeta inteligente DEBERÍA colocar las claves de sesión actualizadas en el archivo de aprovisionamiento EF_LWM2M_Bootstrap.

- Prearranque por medio del enlace UDP, asegurado como se describe en la sección 7.1 (seguridad UDP).

Cuando el enlace UDP no está disponible, el servidor LWM2M (o servidor de arranque) DEBERÍA enviar un SMS al cliente LWM2M para actualizar las claves de sesión antes del siguiente intento de operación "Registrar" o "Actualizar". Si el cliente LWM2M intenta ponerse en contacto con el servidor LWM2M usando un registro caducado, o intenta "Registrar" o "Actualizar" con una clave obsoleta, el servidor LWM2M DEBERÍA responder con un error (petición incorrecta 4.00) y DEBERÍA enviar un SMS para actualizar las claves de sesión. Sin embargo, el servidor LWM2M DEBERÍA enviar dicho SMS antes de que caduque el registro actual, si el cliente LWM2M está activo; o si el cliente LWM2M está en un ciclo de suspensión, el servidor LWM2M (o servidor de arranque) DEBERÍA enviar dicho SMS en la próxima reactivación. Estas medidas evitarán una operación "Registrar" o "Actualizar" fallida.

En cuanto a la sección 7.1 (Seguridad UDP), cuando una sesión persiste durante los ciclos de suspensión, DEBERÍA utilizarse un almacenamiento cifrado y protegido por integridad para las claves y los contadores de la sesión. De forma alternativa, las nuevas claves de sesión DEBERÍAN establecerse mediante uno de los mecanismos anteriores al reactivarse de un ciclo de suspensión.

Preferiblemente, Klc, KID, sPI y TAR DEBERÍAN almacenarse en el recurso "parámetros de clave de enlace de SMS".

Preferiblemente, los valores de clave correspondientes deben almacenarse en el recurso "claves secretas de enlace de SMS".

Un cliente LWM2M que utiliza el enlace de SMS puede proveerse directamente para su uso de un servidor LWM2M de destino (modo de arranque de configuración previa del fabricante) o bien puede arrancar por medio del enlace UDP.

Un cliente, servidor o servidor de arranque LWM2M que admita el enlace de SMS DEBERÍA descartar los mensajes SMS que no estén correctamente protegidos utilizando los parámetros previstos almacenados en el recurso "parámetros de clave de enlace de SMS" y las claves previstas almacenadas en el recurso "claves secretas de enlace de SMS", y NO responderá con un mensaje de error seguro utilizando los parámetros y claves correctos.

Objeto LWM2M: seguridad LWM2M

Descripción: este objeto LWM2M proporciona el material para claves de un cliente LWM2M apropiado para acceder a un servidor LWM2M específico. Una instancia de objeto DEBERÍA dirigirse a un servidor de arranque LWM2M

Estos recursos de objetos LWM2M solo DEBEN modificarse mediante un servidor de arranque LWM2M o aprovisionamiento de tarjeta inteligente y NO DEBEN ser accesibles mediante ningún otro servidor LWM2M.

Información de objeto de ejemplo:

Objeto	ID del objeto	URN del objeto	¿Múltiples instancias?	¿Obligatorio?
Seguridad LWM2M	0		Sí	Sí

Información de recursos:

Nombre del recurso	Tipo	Intervalo o enumeración	Unidades	Descripciones
URI del servidor LWM2M	Cadena	0-255 bytes	-	Identifica de forma única el servidor LWM2M o el servidor de arranque LWM2M y tiene el formato: "coaps://host:port", donde host es una dirección IP o FQDN y port es el puerto UDP del servidor.
Servidor de arranque	Booleano		-	Determina si la instancia actual se refiere a un servidor de arranque LWM2M (verdadero) o a un servidor LWM2M estándar (falso)
Modo de seguridad	Entero	0-3	-	Determina qué modo de seguridad del canal UDP se utiliza 0: Modo de clave precompartida 1: Modo de clave pública sin formato 2: Modo certificado 3: Modo sin seguridad
Clave pública o identidad	Opaco		-	Almacena el certificado del cliente LWM2M (modo certificado), clave pública (modo RPK) o identidad PSK (modo PSK). El formato se define en la sección E.1.1.
Clave pública o identidad del servidor	Opaco		-	Almacena el certificado (modo certificado), la clave pública (modo RPK) o la identidad PSK (modo PSK) del servidor LWM2M o del servidor de arranque LWM2M. El formato se define en la sección E.1.1.
Llave secreta	Opaco		-	Almacena la clave secreta o clave privada del modo de seguridad. El formato del material para claves se define en el modo de seguridad de la sección E.1.1. Este recurso solo DEBE ser modificado por un servidor de arranque y NO DEBE ser legible por ningún servidor.
Modo de seguridad SMS	Entero	0-255	-	Determina qué modo de seguridad de la carga útil de SMS se utiliza (véase la sección 7.2) 0: Reservado para uso futuro 1: Dispositivo en modo de estructura de paquetes seguros terminado 2: Tarjeta inteligente en modo de estructura de paquetes seguros terminada 3: Modo sin seguridad 255: Modos propios
Parámetros de clave de enlace de SMS	Opaco	6 bytes	-	Almacena el Klc, KID, sPI y TAR. El formato se define en la sección D.1.2.
Claves secretas de enlace de SMS	Opaco	32-48 bytes	-	Almacena los valores de las claves para el enlace de SMS. Este recurso solo DEBE ser modificado por un servidor de arranque y NO DEBE ser legible por ningún servidor.
Número de SMS del servidor	Entero			MSISDN utilizado por el cliente LWM2M para enviar mensajes al servidor LWM2M por medio del enlace de SMS. El cliente LWM2M DEBERÍA ignorar

Nombre del recurso	Tipo	Intervalo o enumeración	Unidades	Descripciones
LWM2M				silenciosamente cualquier SMS que no se haya originado en un MSISDN desconocido.
ID de servidor corto	Entero	1-65535	-	Este identificador identifica de forma única cada servidor LWM2M configurado para el cliente LWM2M. Este recurso DEBE establecerse cuando el recurso del servidor de arranque tiene un valor falso. El ID corto por defecto del servidor (es decir, 0) NO DEBE utilizarse para identificar el servidor LWM2M.
Tiempo de espera del cliente	Entero		s	Información pertinente solo para un servidor de arranque. El número de segundos que se deben esperar antes de iniciar un arranque iniciado por el cliente una vez que el cliente LWM2M ha determinado que debe iniciar este modo de arranque.

Seguridad del canal UDP: formato del recurso de clave de seguridad

Esta sección define el formato de la clave secreta, la clave pública y los recursos de identidad del servidor LWM2M y los objetos de arranque LWM2M cuando se utiliza la seguridad del canal UDP. Estos recursos se utilizan para configurar el modo de seguridad y el material para claves que utiliza un cliente con un servidor en particular. Los objetos se configuran en el cliente utilizando uno de los mecanismos de arranque descritos en la sección 5.1 de OMA LWM2M. El uso de este material para claves para cada modo de seguridad se define en la sección 7.1 de OMA LWM2M.

Modo de clave precompartida (PSK)

La PSK es una clave secreta binaria compartida entre el cliente y el servidor de la longitud adecuada para el conjunto de cifrado utilizado [RFC4279]. Esta clave está compuesta por una secuencia de bytes binarios en el recurso de clave secreta. Los conjuntos de cifrado PSK por defecto definidos en esta especificación utilizan una clave AES de 128 bits. Así, esta clave estaría representada en 16 bytes en el recurso de clave secreta.

La identidad PSK correspondiente a esta PSK se almacena en la clave pública o recurso de identidad. La identidad PSK sencillamente se almacena como una cadena UTF-8 según [RFC4279]. Los clientes y servidores DEBEN admitir una identidad PSK de por lo menos 128 bytes de longitud según lo exige [RFC4279].

Modo de clave pública sin formato (RPK)

El modo de clave pública sin formato requiere una clave pública y una clave privada del tipo y longitud adecuados para el conjunto de cifrado utilizado. Estas claves se llevan como una secuencia de bytes binarios con la clave pública almacenada en la clave pública o recurso de identidad y la clave privada almacenada en el recurso de clave secreta. El conjunto de cifrado RPK por defecto definido en esta especificación utiliza una clave ECC de 256 bits. Así, el recurso de certificado contendría una clave pública de 32 bytes y el recurso de clave secreta una clave privada de 32 bytes.

Modo certificado

El modo certificado requiere un certificado X.509v3 junto con una clave privada coincidente. La clave privada se almacena en el recurso de clave secreta como en el modo RPK. El certificado se representa simplemente como binario X.509v3 en el valor de la clave pública o recurso de identidad.

Seguridad de la carga útil de SMS: Formato del recurso de clave de seguridad

Esta sección define el formato de la clave secreta, la clave pública y los recursos de identidad del servidor LWM2M y los objetos de arranque LWM2M cuando se utiliza la seguridad de la carga útil de SMS. Estos recursos se utilizan para configurar el material para claves que un cliente utiliza con un servidor en particular. Los objetos se configuran en el cliente utilizando uno de los mecanismos de arranque descritos en la sección 5.1. El uso de este material para claves se define en la sección 7.2.

Los parámetros de clave de SMS se almacenan en el orden Klc, KID, sPI, TAR (Klc es el byte 0).

El orden de los bits dentro de los bytes DEBERÍA seguir las "convenciones de codificación" de ETSI TS 102 221 (b8 MSB, b1 LSB).

Desarranque

Si se va a eliminar una instancia de objeto de seguridad, es necesario eliminar o modificar algunos recursos y configuraciones relacionados. Por lo tanto, cuando la operación de eliminación se envía por medio de la interfaz de arranque, el cliente DEBE continuar con el procedimiento siguiente.

1. Si existe una instancia de objeto a la que solo puede acceder un servidor de la instancia de objeto de servidor (es decir, el servidor es el propietario del control de acceso y el servidor LWM2M puede acceder a la instancia del objeto solo en una instancia del objeto de control de acceso), la instancia del objeto y la correspondiente instancia del objeto de control de acceso DEBEN eliminarse

2. Si múltiples servidores pueden acceder a una instancia de objeto, incluido el servidor cuya instancia de objeto de seguridad se va a eliminar, entonces:

- Se DEBE eliminar una instancia de recurso ACL para el servidor en la instancia del objeto de control de acceso para la instancia del objeto.

- Si el servidor es el propietario del control de acceso de la instancia del objeto de control de acceso, entonces el propietario del control de acceso DEBE cambiarse a otro servidor según las reglas siguientes: El cliente DEBE elegir el servidor que tenga la suma más alta de cada número asignado a un derecho de acceso (escribir: 1, eliminar: 1) para el propietario del control de acceso. Si dos o más servidores tienen la misma suma, el cliente DEBE elegir uno de ellos como propietario del control de acceso.

3. La observación del servidor DEBE eliminarse

4. La instancia del objeto del servidor DEBE eliminarse

5. El cliente PUEDE enviar la operación "cancelar registro" al servidor

Nota: para supervisar el cambio de propietario del control de acceso, el servidor PUEDE observar el recurso del propietario del control de acceso.

Como mejora adicional, la GBA BSF se puede fusionar con el servidor de arranque LWM2M. Esto hace que sea más fácil detectar un único servidor. Esto se muestra en la figura 5 en la que un servidor combinado 420 contiene tanto la BSF 130 como el LWM2M 440.

Extensiones para su uso con soluciones de clave pública

Un problema con las claves derivadas con GBA es que se basan en el secreto a largo plazo de la clave (U)SIM subyacente, K o Ki. Si esa clave alguna vez se filtra en el futuro, o si el operador se ve obligado a revelarla por algún motivo, entonces cualquier clave derivada que alguna vez se haya utilizado en GBA puede considerarse comprometida. Un adversario o una tercera parte que haya estado grabando todas las conversaciones con un dispositivo puede potencialmente recuperar todas las claves y mensajes anteriores protegidos por ellas.

Una solución para esto es asegurar que las claves GBA solo se utilizan temporalmente al inscribirse en un esquema de clave pública: ese esquema puede, por ejemplo, admitir un "secreto directo perfecto", que evita el problema de que la clave se comprometa en el futuro y conlleve a una recuperación de todos los mensajes cifrados.

El estándar del 3GPP (GAA) proporciona algunos procedimientos para utilizar GBA para inscribirse en certificados de clave pública. Sin embargo, son particularmente complejos y la infraestructura de clave pública (PKI) necesaria puede ser una sobrecarga demasiado grande para LWM2M u otros protocolos M2M.

Autenticar claves públicas "sin formato" del cliente:

El dispositivo M2M puede tener un par de claves pública-privada precargado o puede generar un par de claves pública-privada en el primer encendido. Presenta su "clave pública sin formato" (o una función hash de la clave pública sin formato) a la BSF, protegida mediante autenticación implícita HTTP y RES (esto podría ser a través de un protocolo Ub tunelizado, puesto que eso ya requiere cierta personalización). De forma alternativa, la clave pública sin formato se puede presentar a la NAF (servidor LWM2M o servidor de arranque LWM2M) protegida con la clave Ks_NAF derivada del GBA. (El dispositivo podría, por ejemplo, presentar su clave pública sin formato por medio de CoAP, protegida por integridad mediante la Ks_NAF, o presentarla dentro de una sesión CoAP segura utilizando un conjunto de cifrado de clave precompartida y la Ks_NAF).

El servidor DM (o servidor de arranque) puede entonces utilizar uno de los conjuntos de cifrado de clave pública, tal como:

- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 como se define en la sección 9.1.3.2 de [CoAP]
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 como se define en [RFC5289]

De forma alternativa, el servidor DM puede utilizar un conjunto de cifrado mixto de clave precompartida/clave pública como:

- TLS ECDHE PSK CON AES 128 CBC SHA256, como se define en [RFC5489] utilizando la Ks_NAF como clave precompartida.

Preferiblemente, estos conjuntos de cifrado pueden proporcionar un secreto directo perfecto. Es posible que se puedan llevar a cabo varios procedimientos antes de que se establezca una Ks_NAF. En particular, estos procedimientos se pueden llevar a cabo para dispositivos que no admiten GBA o donde la tarjeta SIM del dispositivo M2M aún no está provista para GBA.

El dispositivo puede presentar su clave pública sin formato sin autenticar y el servidor DM o de arranque pueden aceptar esta clave pública sin formato temporalmente. El dispositivo puede utilizar un secreto débil (como PIN+IMSI+IMEI) junto con TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256, por ejemplo, para asegurar una primera conexión con un servidor de arranque.

Estos procedimientos de respaldo no proporcionan una autenticación (o proporcionan una autenticación débil) de la clave pública del dispositivo, pero por lo menos permiten que el protocolo se inicie, incluido proveer la conectividad para hacer un túnel GBA o ejecutar una inserción de GBA, y así establecer una autenticación sólida posterior de la clave pública del dispositivo.

Autenticar claves públicas "sin formato" del servidor.

Como alternativa, o además del procedimiento mencionado anteriormente para autenticar claves públicas "sin formato" del cliente, el servidor DM puede presentar su propia "clave pública sin formato" al cliente, protegida por autenticación implícita HTTP y RES, u otras técnicas, o mediante una comprobación de integridad o una sesión PSK establecida con la clave Ks_NAF derivada del GBA, por ejemplo. También se pueden utilizar conjuntos de cifrado parecidos a los descritos anteriormente para proporcionar un secreto directo perfecto.

Si no ha habido oportunidad de establecer una Ks_NAF, entonces el dispositivo puede requerir una copia precargada o un resumen de la clave pública prevista (p. ej., la clave pública utilizada por el servidor de arranque LWM2M) o un secreto débil precargado. Este resumen o secreto se puede recuperar de la tarjeta SIM (UICC) para evitar la necesidad de proveerlo directamente al dispositivo en el momento de la fabricación. Como alternativa, puede enviarse al dispositivo por SMS o el dispositivo puede aceptar la clave pública del servidor sin autenticar, por lo menos en la primera conexión.

Nuevamente, procedimientos de respaldo no proporcionan una autenticación (o proporcionan una autenticación débil) de la clave pública del servidor, pero por lo menos permiten que el protocolo se inicie, incluido proveer la conectividad para hacer un túnel GBA o ejecutar una inserción de GBA, y así establecer una autenticación sólida posterior de la clave pública del servidor.

Las técnicas mencionadas anteriormente para autenticar claves públicas "sin formato" del cliente también pueden aplicarse a modos certificado, p. ej., en lugar de una clave pública sin formato, el dispositivo puede presentar un certificado autofirmado (o un certificado firmado por una CA desconocida). El servidor puede presentar un certificado autofirmado o un certificado de CA de raíz desconocida al dispositivo M2M. Esto también evita la complejidad y el gasto de proveer el dispositivo M2M en el momento de la fabricación de un certificado de clave pública firmado por una CA preexistente (p. ej., la CA del fabricante del dispositivo) o proveer múltiples certificados raíz.

Estas realizaciones también permiten la actualización frecuente de claves o certificados privados/públicos, lo que soluciona algunos problemas de revocación. Sin embargo, no es necesario realizar una comprobación de la revocación, ya que la clave pública/privada no dura mucho. La duración de la clave pública/privada puede estar vinculada a la duración de un B-TID (o clave LT).

De forma alternativa, el GBA podría utilizarse para asegurar mensajes de una fuente de tiempo fiable (p. ej., un tiempo de la red) o proporcionar un canal seguro para recuperar información de validación de certificado (respuestas CRL o OCSP). Esto puede solucionar algunos problemas con la obtención de información correcta y actualizada para la validación del certificado.

La figura 8 muestra un diagrama de flujo de un procedimiento 600 para comunicarse de forma segura con un dispositivo M2M de una manera que protege el secreto de las comunicaciones a largo plazo. En la etapa 610 se obtiene un secreto compartido. Esto puede generarse o recuperarse del almacenamiento. Además, el secreto compartido puede obtenerse del dispositivo M2M, el servidor u otra fuente. El secreto compartido (o los datos derivados del secreto compartido, tal como su función hash) se comparten entre el dispositivo M2M y el servidor. Esto puede ser por simple transmisión, SMS u otro mecanismo, por ejemplo. También puede tener lugar la autenticación por parte del dispositivo y/o servidor M2M y puede utilizar el secreto compartido.

Se establece, se asegura o se inicia una conexión entre el dispositivo M2M y el servidor en la etapa 630. Esta conexión utiliza el secreto compartido o los datos derivados. Puede haber algún tipo de seguridad o autenticación débil (p. ej., contraseña, PIN, IMSI y/o secreto derivado de IMEA) o ninguna seguridad o autenticación implicada en la conexión. Sin embargo, el secreto compartido ahora puede utilizarse para establecer el material criptográfico entre el dispositivo M2M y el servidor en la etapa 640. En otras palabras, la conexión puede tener poca o ninguna seguridad y el secreto compartido puede tener un nivel de seguridad bajo o inferior (en comparación con el material criptográfico) pero, no obstante, puede utilizarse para proporcionar el material criptográfico correspondiente en el dispositivo y servidor M2M. El material criptográfico puede utilizarse para asegurar la comunicación entre el dispositivo M2M y el servidor (etapa

650). Esta comunicación segura utiliza un protocolo criptográfico (p. ej., TLS o SSL) y preferiblemente un protocolo criptográfico que proporciona un secreto directo perfecto. El dispositivo M2M y el servidor ahora pueden comunicarse de forma segura.

El secreto compartido puede ser una clave pública de un par de clave privada y clave pública, o un certificado (incluido el autofirmado, el firmado por una autoridad certificadora conocida o el firmado por una autoridad certificadora desconocida), por ejemplo.

Preferiblemente, el secreto compartido (p. ej., clave o certificado) está configurado para que caduque o se actualice a intervalos (p. ej., cada uno, dos, tres o más días). El material criptográfico puede ser de tipo parecido o diferente al secreto compartido. Puede ser más seguro y también puede tener un tiempo de caducidad (aunque puede ser diferente al del secreto compartido).

La figura 9 ilustra esquemáticamente un sistema 700 que se utiliza para implementar el procedimiento 600 descrito en referencia a la figura 8. El sistema incluye un servidor 720 que incluye lógica 730 para llevar a cabo el procedimiento. Uno o más dispositivos 110 M2M se comunican a través de conexiones con el servidor 720 de la manera descrita anteriormente. Los dispositivos M2M también incluyen la lógica 710 utilizada para implementar el procedimiento. En la realización que se muestra en la figura 9, cada dispositivo 110 M2M tiene una única conexión con el servidor 720. En esta implementación, la comunicación segura se puede asegurar a través de esta conexión (típicamente) no segura. Sin embargo, en otras realizaciones se puede utilizar una conexión separada (del mismo o de diferente tipo) para que tenga lugar la comunicación segura.

En las realizaciones en las que el servidor 720 genera o recupera el secreto compartido (p. ej., clave o certificado), entonces su propia lógica 730 llevará a cabo esta tarea. En las realizaciones en las que el dispositivo 110 M2M genera o recupera el secreto compartido (p. ej., clave o certificado), su propia lógica 710 llevará a cabo esta tarea.

A continuación, se describen usos particulares de la seguridad directa perfecta y la autenticación de procedimientos de clave pública sin formato u otros procedimientos de comunicación seguros. Estos incluyen actualizaciones de firmware seguras y radiodifusiones seguras.

Es posible que a un dispositivo cliente M2M se le notifique una clave pública del lado del servidor diferente. Esta clave pública diferente se puede utilizar para firmar actualizaciones de firmware (a través de un sistema de unidifusión, radiodifusión o multidifusión o entre pares, por ejemplo).

Esta funcionalidad puede extenderse a otros tipos de radiodifusión segura, por ejemplo, distribuir una clave pública para firmar mensajes de advertencia públicos (alertas de bomba, alertas de tsunami), mensajes de emergencia (ambulancia acercándose, apártese), alertas de tráfico, etc.

Este procedimiento tiene las ventajas de una PKI reducida o nula, y de una validación de certificados nula o más sencilla. Se puede enviar una clave pública (protegida por una clave establecida mediante GBA) donde luego se utiliza la clave pública para verificar mensajes de radiodifusión o actualizaciones de firmware, por ejemplo.

La especificación LWM2M no tiene un canal de radiodifusión y las actualizaciones de firmware en LWM2M funcionan de la siguiente manera:

- El servidor LWM2M realiza una operación de "escritura" (o "creación") para modificar (o crear una nueva instancia de) un objeto de "actualización de firmware". Puede escribir la actualización en un recurso "paquete", pero dado que las actualizaciones suelen ser grandes (y difíciles de llevar a través de CoAP), lo más probable es que escriba un URI en el recurso "URI del paquete".

- Si se ha escrito el recurso "URI del paquete", entonces el cliente LWM2M "realiza la descarga en la próxima oportunidad práctica". Durante la descarga, el cliente LWM2M establece el recurso "estado" en "2" (que significa "descarga"). Al finalizar la descarga, el cliente LWM2M establece el recurso "estado" en "3" (que significa "descargado"). Si el recurso "paquete" se ha escrito directamente, cuando el cliente LWM2M haya completado la operación de escritura, establecerá el recurso "estado" en "3" inmediatamente.

- El servidor LWM2M puede realizar una operación de "lectura" cuando lo desee para conocer el valor del "estado". Cuando el estado es "3", puede realizar una operación "ejecutar" en el recurso "actualizar", que indica al cliente LWM2M que instale la actualización del firmware.

- El cliente LWM2M configura el recurso "resultado de la actualización" para indicar si la actualización se ha realizado correctamente o no y cualquier motivo del error. El cliente también establece el recurso "estado" nuevamente en "1" (que significa "inactivo").

- El servidor LWM2M puede realizar otra operación de "lectura" cuando lo desee para conocer el valor de los recursos "resultado de actualización" y "estado".

En este proceso no se produce ninguna verificación del paquete de actualización.

Sin embargo, a continuación, se describen mejoras de este procedimiento. Estas se ilustran en dos mecanismos de ejemplo. En estos ejemplos, se incluye una clave dentro de las operaciones LWM2M.

Mecanismo 1 El servidor LWM2M realiza una operación de "escritura" en el recurso "paquete", pero en lugar de escribir la actualización del firmware en sí, escribe la clave (típicamente pública) que el cliente LWM2M requiere para verificar la actualización del firmware. El servidor LWM2M realiza simultáneamente (o secuencialmente) una operación de "escritura" en el recurso "URI del paquete", que indica al cliente LWM2M dónde puede encontrar la actualización.

NOTA: el URI aquí bien puede adoptar la forma de un URI de radiodifusión, por ejemplo (véase htttp://tools.ietf.org/html/rfc2838) o http://www.etsi.org/deliver/etsi_ts/102800_102899/102851/01.01.01_60/ts_102851v010101p.pdf

Una vez que el cliente LWM2M ha descargado la actualización, podrá verificarla mediante la clave pública escrita en el recurso "paquete".

Mecanismo 2 El servidor LWM2M realiza una operación de "escritura" en el recurso "URI del paquete", pero el URI contiene una codificación de la clave pública que será necesaria para verificar la actualización del firmware. Por ejemplo, adopta la forma de:

dvb://channel135/key=9ICYfQ4RHZO3a3jb6hrQWRQiga7ImCqCaG9JemD7F6r

Una vez que el cliente LWM2M ha descargado la actualización, podrá verificarla mediante la clave pública contenida en el recurso "URI del paquete".

Se puede usar una clave establecida por GBA para asegurar una sesión entre el cliente LWM2M y el servidor LWM2M (por ejemplo, la Ks_NAF se utiliza como una clave precompartida DTLS) y luego se proporciona la segunda clave dentro de esa sesión segura.

En un ejemplo, los medidores de gas residenciales pueden requerir actualizaciones de firmware (p. ej., se detecta un error que significa que informarán incorrectamente el gas consumido. Es posible que los piratas informáticos intenten aprovechar esto y se requiera un parche). El operador de telefonía móvil ofrece algunas capacidades de radiodifusión en su red, por ejemplo, por medio de MBMS. Uno de los canales de radiodifusión es "gratuito" (es decir, no está cifrado) pero consiste en un flujo de actualizaciones de firmware para muchos tipos de dispositivos M2M (medidores de gas, medidores de electricidad, sistemas de gestión de motores, etc.) Cada actualización puede estar firmada con una clave privada separada y los pares de claves pueden actualizarse periódicamente (para asegurar que solo las actualizaciones más recientes estén firmadas con las claves más recientes).

La vez siguiente que cada medidor de gas se pone en contacto con el servidor de gestión de dispositivos, se le proporciona una clave pública autenticada. La clave pública puede ser protegida por integridad utilizando el secreto compartido (Ks NAF) que se ha establecido entre el medidor de gas y el servidor de gestión de dispositivos M2M mediante GBA. Luego, el medidor de gas supervisa el canal de radiodifusión MBMS para detectar cuándo se radiodifunde una actualización y cuál se ha firmado con la clave privada correspondiente. Descarga la actualización, la verifica utilizando la clave pública y, si está verificada, instala la actualización.

En otro ejemplo de implementación, una organización de una tercera parte (comercial, gubernamental o no comercial, por ejemplo) puede desear introducir uno o varios servicios nuevos y estos servicios pueden clasificarse por tipo de dispositivo y categoría de dispositivo (es decir, alertas de tráfico en la carretera puede ser un tipo de alerta de información que tiene una categoría de dispositivo como transporte. Un sistema de aviso de tsunami puede ser del tipo mensaje de emergencia de seguridad pública y la categoría de dispositivo "todos". Este sistema de categorización taxonómica de dispositivos puede perfeccionarse aún más para asegurar que los anuncios de servicios se encaminan a los dispositivos apropiados.)

La organización de la tercera parte puede informar a un proveedor de servicios (por ejemplo, un proveedor de servicios de telecomunicaciones) del servicio. El proveedor de servicios puede validar el servicio y puede utilizar el mecanismo descrito anteriormente en relación con la radiodifusión segura de mensajes para distribuir una descripción del servicio a los dispositivos.

Este servicio podría utilizarse de forma recursiva para informar sobre otros anunciantes de servicios. En otras palabras, el proveedor de servicios podría anunciar la existencia de un organismo regulador (una agencia gubernamental) que podría estar autorizado a anunciar servicios gubernamentales.

Estos servicios podrán ser de tres tipos: optativo, de exclusión voluntaria y obligatorio. En otras palabras, un servicio con fines de seguridad nacional anunciado por una agencia gubernamental puede ser obligatorio, un servicio de alertas de tráfico proporcionado por una empresa comercial puede ser optativo y un servicio anunciado por una agencia gubernamental con fines de seguridad pública puede ser de exclusión voluntaria.

En otro ejemplo, una organización de una tercera parte (comercial, gubernamental o no comercial) puede desear

introducir uno o más servicios nuevos. Estos servicios pueden clasificarse por tipo de dispositivo y categoría de dispositivo (es decir, las alertas de tráfico en carretera serían de tipo alerta de información y la categoría de dispositivo de transporte, el sistema de aviso de tsunami sería del tipo mensaje de emergencia de seguridad pública y la categoría de dispositivo, todos. Este sistema taxonómico de categorización de dispositivos podría perfeccionarse aún más para asegurar que los anuncios de servicios se encaminen a los dispositivos apropiados).

La organización de la tercera parte podrá informar del servicio a un operador de red de telecomunicaciones. El operador de red puede validar el servicio y puede utilizar el procedimiento de comunicación con dispositivos M2M descrito anteriormente para distribuir una descripción del servicio a los dispositivos.

Este servicio podría utilizarse de forma recursiva para informar sobre otros anunciantes de servicios. En otras palabras, un operador de red podría anunciar la existencia de un organismo regulador (es decir, una agencia gubernamental) que podría estar autorizado a anunciar servicios gubernamentales, por ejemplo.

Los servicios de ejemplo pueden ser de tres tipos en general: optativo/de exclusión voluntaria/obligatorio. Por ejemplo, un servicio con fines de seguridad nacional anunciado por una agencia gubernamental sería obligatorio, un servicio de alertas de tráfico proporcionado por una empresa comercial sería opcional y un servicio anunciado por una agencia gubernamental con fines de seguridad pública podría ser de exclusión voluntaria.

Un ejemplo de uso de claves GBA es proteger un SMS (cifrar/proteger la integridad de los SMS mediante una interfaz de paquetes segura, p. ej., como ETSI TS 102.225 que se utiliza para SIM OTA). Es probable que este canal de SMS sea más eficaz que DTLS.

Actualmente falta la funcionalidad de SMS cifrados en OMA LWM2M. En otras implementaciones, se puede utilizar un protocolo SMS seguro con un protocolo de gestión de dispositivos. Por ejemplo:

a) Utilizar un protocolo SMS seguro, originalmente diseñado para SIM OTA (102 225), pero actualmente adaptado para las comunicaciones LWM2M, y

b) Utilizar el protocolo LWM2M para definir (y gestionar) los parámetros necesarios para un protocolo SMS seguro, p. ej., el Klc, KID, sPI, TAR y claves pertinentes.

El uso de GBA se convierte entonces en una extensión adicional de esta idea, ya que se utiliza para derivar las claves de forma segura.

En un ejemplo particular, un sistema de termostato industrial (p. ej., en un almacén) puede tener la temperatura establecida de forma remota por medio de un servidor de gestión de dispositivos. Dado que los datos de temperatura son muy cortos (solo un número en grados Celsius), entonces (o cualquier otro dato) se puede transmitir en un solo SMS, por ejemplo, usando el protocolo OMA LWM2M con un portador de SMS.

Por lo tanto, es necesario proteger el SMS para impedir manipulaciones maliciosas del termostato (u otros equipos que puedan depender de datos de sensores o parámetros) y posibles daños a los bienes almacenados en el almacén, facturas de energía innecesarias, etc. El SMS puede ser cifrado y protegido por integridad utilizando el protocolo de paquete seguro descrito en ETSI TS 102 225. Primero, el GBA se utiliza para establecer una KS_NAF entre el termostato y el servidor LWM2M. Para mayor comodidad, se puede utilizar un SMS inicial para entregar un mensaje GPI (información de inserción de GBA) desde el servidor LWM2M al termostato.

Este GPI contiene una pregunta de autenticación para pasar a una tarjeta SIM (UICC), que podría estar en el termostato o quizás en otro lugar de la red del almacén (podría estar en un centro de comunicaciones). La aplicación USIM de la tarjeta SIM procesa la pregunta y se devuelven un CK y un IK.

Luego se utilizan para derivar la Ks y luego la Ks_NAF que se pasa al termostato. Luego, el termostato (u otro equipo) extrae las claves para el Kc y Kid y las almacena para que las utilice el cliente LWM2M en el termostato. Una solución podría ser la siguiente: la Ks_NAF es de 256 bits (o número total de bits); los primeros 128 bits (o conjunto de bits) se utilizan como clave de cifrado AES (para el Kc) y los últimos 128 bits (o conjunto de bits siguiente o final) se utilizan como clave de integridad (para el Kid). Una vez se ha establecido esto, se puede enviar un SMS cifrado y protegido por integridad con la temperatura deseada siempre que sea necesario desde el servidor LWM2M al cliente LWM2M en el termostato. Luego, el cliente descifra y verifica la temperatura deseada, y el termostato establece esa temperatura (o el dispositivo cambia un ajuste o parámetro en particular).

Conjunto de pruebas automatizado.

En esta implementación de ejemplo, los proveedores de servicios de valor añadido pueden utilizar un conjunto de pruebas automatizado que podría utilizarse para proporcionar suministrar de mantenimiento adicionales (en este caso, diagnóstico y análisis de rendimiento) con el fin de asegurar un comportamiento óptimo del dispositivo. Típicamente, este sería un servicio ofrecido por el proveedor del dispositivo original como un servicio de valor añadido. Sin embargo, es viable que proveedores de servicios especializados puedan suministrar estos servicios (p. ej., servicio de mantenimiento/puesta a punto de automóviles). El beneficio para el proveedor de equipos es que genera ingresos y

oportunidades de venta. Otro caso de uso sería cuando existiera un ecosistema de dispositivos complejo (p. ej., una red de área doméstica (HAN) con muchos dispositivos periféricos de diferentes tipos). Un proveedor de servicios de mantenimiento HAN tendría (o crearía) datos de firma para un funcionamiento correcto e incorrecto de los dispositivos compatibles y proporcionaría servicios de diagnóstico para esos dispositivos.

Otros canales de mensajería (y esto es aplicable a todos los ejemplos descritos) podrían ser DSL y wifi convencionales, donde hubiera un bajo nivel de seguridad en la infraestructura física y fueran fáciles de interceptar e interferir con las comunicaciones.

Uso de GBA para enviar un mensaje seguro que inicia una autoprueba/prueba de diagnóstico del dispositivo. Esto cubre la funcionalidad LWM2M o funcionalidad general. Los resultados de la autoprueba también pueden informarse de vuelta mediante un mensaje de GBA seguro. Esto podría basarse en la seguridad de los SMS, como se describe en Idea 16, o utilizar un canal de mensajería diferente.

Por motivos de rendimiento y gestión energética, no queremos que cualquiera pueda desencadenar una autoprueba, por lo que este debería ser un mensaje seguro. Asimismo, por motivos de privacidad y seguridad, no queremos que los resultados de la autoprueba se revelen a nadie que los solicite. Sin embargo, es poco probable que alguien alguna vez establezca una seguridad especial y fuerte solo para hacer esto. Por lo tanto, es un buen caso de uso para GBA a diferencia de otras arquitecturas de seguridad.

Venta al final del servicio y retirada del dispositivo.

Esta implementación de ejemplo ilustra la capacidad de crear una relación de confianza entre dispositivos y proveedores de servicios, crea oportunidades para ofrecer servicios de seguridad a todos los dispositivos de forma simétrica. Por ejemplo, se puede utilizar una tostadora como aparato electrodoméstico para facilitar que un usuario vote en unas elecciones gubernamentales, y un monedero electrónico puede adquirir información sobre el tráfico rodado. Los servicios de seguridad se pueden ofrecer de forma independiente al dispositivo. En los casos de fin del servicio, la autorización para que el dispositivo participe en una subasta para venderse y/o conseguir un reemplazo se proporcionaría por el propietario del aparato electrodoméstico (por algún medio), y la responsabilidad de participar en una puja/venta por subasta se delegaría al dispositivo en cuestión.

Una vez establecida la relación de confianza, se crea una oportunidad para añadir valor. En el caso del fin del servicio, esto podría incluir proporcionar historiales de vida/servicio a compradores potenciales o planificar la recogida del dispositivo para su eliminación y reciclaje.

El dispositivo puede utilizar una asociación segura establecida mediante GBA para listarse en eBay por sí mismo, por ejemplo, y pedir una sustitución.

Este tipo de aplicaciones automatizadas de pedidos y ventas requieren una gran seguridad. Por lo tanto, este es un buen uso de la implementación de GBA descrita en particular.

Llavero de seguridad

Esta implementación de ejemplo describe un mecanismo para transferir material protegido de seguridad de forma asimétrica, desde un dispositivo seguro que utiliza GBA, a un dispositivo (potencialmente) no seguro. Se pueden dar muchos ejemplos para este caso de uso utilizando la analogía del llavero. Estas transferencias pueden ser automatizadas o bajo el control del usuario o una combinación de ambas.

Una extensión adicional de esto sería el uso simétrico donde dos dispositivos compatibles con GBA no relacionados necesitan intercambiar información (como se describe en el documento WO2012/035340).

Los dispositivos reconocen la presencia y la identidad de cada uno (es decir, tienen visibilidad entre sí, tal como un automóvil que pasa por una cabina de peaje. La cabina de peaje podría usar un bucle de inducción para detectar la presencia de un automóvil y utilizar Bluetooth/ RFID (u otro sensor) para suministrar otra información en texto simple, por ejemplo) y adquiriría información de firma del otro dispositivo. Cada dispositivo comunica por medios seguros a su plataforma de gestión de dispositivos la existencia del otro dispositivo + las credenciales de seguridad + las firmas de seguridad (recibidas y dadas). Las plataformas de gestión de dispositivos (que tendrían una relación de confianza preexistente entre sí tal como, por ejemplo, por medio de certificados de CA fiables) luego validan las firmas proporcionadas para cada dispositivo y negocian las claves de seguridad para admitir la comunicación entre los dispositivos. (Esta puede ser una clave simétrica simple). Las claves derivadas se envían a los dispositivos y luego los dispositivos pueden comunicarse entre sí de forma segura e iniciar una transferencia monetaria (por ejemplo).

Se ha de entender que la descripción anterior se proporciona a modo de ejemplo y solo para el beneficio de comprender la solución, y debe incluir también cualquier combinación de las características anteriores, así como cualquier alteración, modificación o en cualquier caso adición que pueda ser realizada por un experto en la materia mediante el uso de sus habilidades y/o conocimientos generales en la técnica pertinente y/o relacionada.

Muchas combinaciones, modificaciones o alteraciones de las características de las realizaciones anteriores serán

fácilmente evidentes para el experto en la materia y están destinadas a formar parte de la invención. Cualquiera de las características descritas específicamente relacionada con una realización o ejemplo se puede utilizar en cualquier otra realización realizando los cambios apropiados.

REIVINDICACIONES

1. Un procedimiento para comunicarse de forma segura con un dispositivo (110) de máquina a máquina, M2M, que comprende las etapas de:

compartir un secreto o los datos derivados del secreto entre el dispositivo (110) M2M y un servidor (120);

establecer una conexión entre el dispositivo (110) M2M y el servidor (120);

utilizar el secreto compartido o los datos derivados del secreto compartido para establecer el material criptográfico en el servidor (120); y

asegurar la comunicación entre el dispositivo (110) M2M y el servidor (120) con un protocolo criptográfico que utiliza el material criptográfico establecido, en el que el material criptográfico es irrecuperable a partir del secreto compartido o de los datos derivados únicamente del secreto compartido,

en el que la etapa de utilizar el secreto compartido o los datos derivados del secreto compartido para establecer el material criptográfico comprende además las etapas de:

el servidor (120) genera u obtiene una clave pública y una clave privada correspondiente;

el servidor (120) autentica una clave pública del dispositivo (110) M2M utilizando el secreto compartido o los datos derivados del secreto compartido; y

derivar el servidor (120) el material criptográfico a partir de la clave pública del dispositivo (110) M2M y la clave privada del servidor (120).

2. Un procedimiento para comunicarse de forma segura con el servidor (120) que comprende las etapas de:

compartir un secreto o los datos derivados del secreto entre el servidor (120) y un dispositivo (110) de máquina a máquina, M2M;

establecer una conexión entre el dispositivo (110) M2M y el servidor (120);

utilizar el secreto compartido o los datos derivados del secreto compartido para establecer el material criptográfico en el dispositivo (110) M2M; y

asegurar la comunicación entre el dispositivo (110) M2M y el servidor (120) con un protocolo criptográfico que utiliza el material criptográfico establecido, en el que el material criptográfico es irrecuperable a partir del secreto compartido o de los datos derivados únicamente del secreto compartido,

en el que la etapa de utilizar el secreto compartido o los datos derivados del secreto compartido para establecer el material criptográfico comprende además las etapas de:

el dispositivo (110) M2M genera u obtiene una clave pública y una clave privada correspondiente;

el dispositivo (110) M2M autentica una clave pública del servidor (120) utilizando el secreto compartido o los datos derivados del secreto compartido; y

el dispositivo (110) M2M deriva el material criptográfico a partir de la clave pública del servidor (120) y la clave privada del dispositivo (110) M2M.

3. El procedimiento de la reivindicación 1, en el que la etapa de autenticar la clave pública del dispositivo (110) M2M emplea una comunicación entre un servidor de arranque y el dispositivo (110) M2M y/o una comunicación entre el servidor y el servidor de arranque.

4. El procedimiento según cualquier reivindicación anterior, en el que el material criptográfico son claves de sesión para proporcionar un secreto directo perfecto.

5. El procedimiento según cualquier reivindicación anterior, en el que el protocolo criptográfico es seguridad de la capa de transporte, TLS, capa de conexión segura, SSL o seguridad de la capa de transporte de datagramas, DTLS.

6. El procedimiento según cualquier reivindicación anterior, en el que el servidor (120) es un servidor de gestión de dispositivos, un servidor de arranque de gestión de dispositivos, un servidor de M2M de baja complejidad, LWM2M, un servidor de arranque LWM2M o una función de aplicación de red, NAF.

7. El procedimiento según cualquier reivindicación anterior, en el que el servidor (120) es una función de servidor de arranque, BSF.

8. El procedimiento según cualquier reivindicación anterior, en el que la comunicación segura entre el dispositivo (110)

M2M y el servidor se realiza a través de la conexión.

9. El procedimiento de la reivindicación 8, en el que la etapa de asegurar la conexión entre el dispositivo (110) M2M y el servidor (120) comprende además proporcionar mensajes de arquitectura de arranque genérico, GBA, o de información de inserción de GBA, GPI, a través de la conexión.

10. El procedimiento según cualquier reivindicación anterior, en el que el secreto compartido se utiliza para establecer, proteger, respaldar o autenticar un certificado, un certificado autofirmado o un certificado firmado por una autoridad certificadora desconocida o no verificable.

11. El procedimiento según cualquier reivindicación anterior, en el que el secreto compartido se utiliza para establecer, proteger, respaldar o autenticar una clave o certificado de autoridad, y en el que la clave de autoridad se utiliza para firmar, respaldar o autenticar un certificado o clave pública para el dispositivo (110) y/o servidor (120).

12. El procedimiento según cualquier reivindicación anterior, en el que el secreto compartido se utiliza para verificar que una clave pública o un certificado todavía es válido.

13. El procedimiento según cualquier reivindicación anterior, en el que el secreto compartido se utiliza para autenticar un certificado o clave pública actualizada.

14. Un dispositivo (110) de máquina a máquina, M2M, que comprende:

lógica configurada para:

compartir un secreto o los datos derivados del secreto entre el dispositivo (110) M2M y un servidor (120);

establecer una conexión entre el dispositivo (110) M2M y el servidor (120); utilizar el secreto compartido o los datos derivados del secreto compartido para establecer el material criptográfico en el dispositivo (110) M2M; y

asegurar la comunicación entre el dispositivo (110) M2M y el servidor (120) con un protocolo criptográfico que utiliza el material criptográfico establecido, en el que el material criptográfico es irrecuperable a partir del secreto compartido o de los datos derivados únicamente del secreto compartido, en el que:

el dispositivo (110) M2M está configurado para generar u obtener una clave pública y una clave privada correspondiente;

el dispositivo (110) M2M está configurado para autenticar una clave pública del servidor (120) utilizando el secreto compartido o los datos derivados del secreto compartido; y

el dispositivo (110) M2M está configurado para derivar el material criptográfico a partir de la clave pública del servidor (120) y la clave privada del dispositivo (110) M2M.

15. Un servidor (120) que comprende:

lógica configurada para:

compartir un secreto o los datos derivados del secreto entre el servidor (120) y un dispositivo (110) de máquina a máquina, M2M;

establecer una conexión entre el servidor (120) y el dispositivo (110) M2M; utilizar el secreto compartido o los datos derivados del secreto compartido para establecer el material criptográfico en el servidor (120); y

comunicación segura entre el servidor (120) y el dispositivo (110) M2M con un protocolo criptográfico que utiliza el material criptográfico establecido, en el que

el material criptográfico es irrecuperable a partir del secreto compartido o de los datos derivados únicamente del secreto compartido, en el que:

el servidor (120) está configurado para generar u obtener una clave pública y una clave privada correspondiente;

el servidor (120) está configurado para autenticar una clave pública del dispositivo (110) M2M utilizando el secreto compartido o los datos derivados del secreto compartido; y

el servidor (120) está configurado para derivar el material criptográfico a partir de la clave pública del dispositivo (110) M2M y la clave privada del servidor (120).

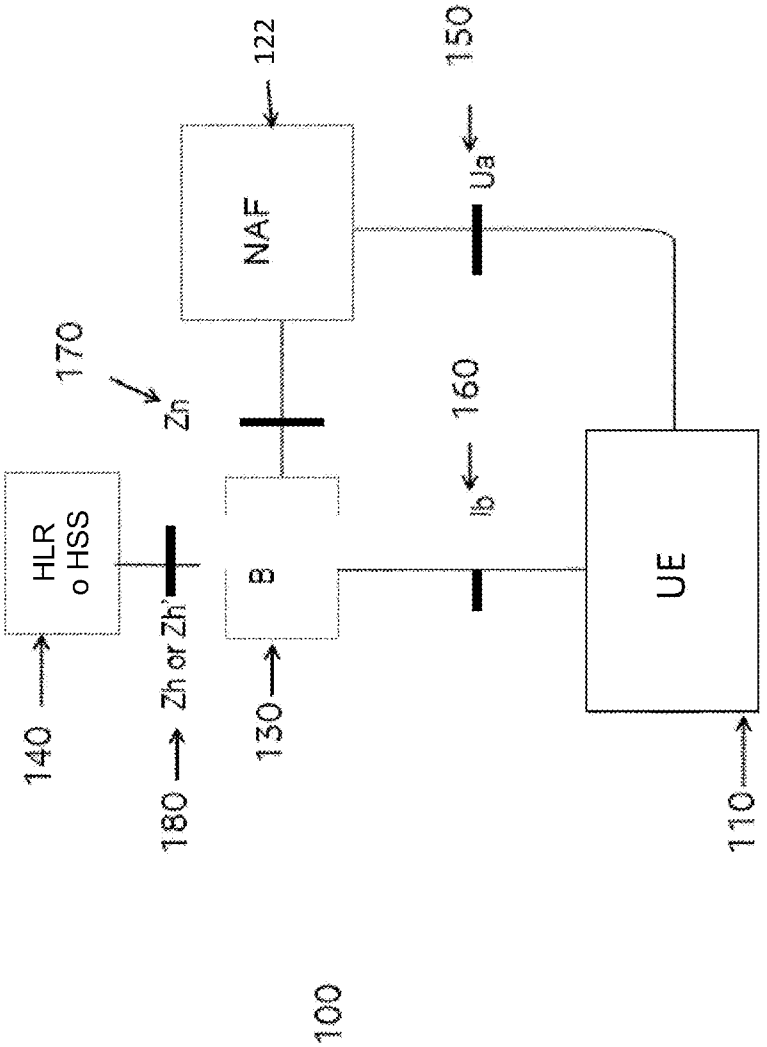

122
150
NAF
Ua
170
Zn
160
Ib
HLR
o HSS
B
UE
Zh or Zh'
140
130
180
110
100

FIG. 1

Fig. 1

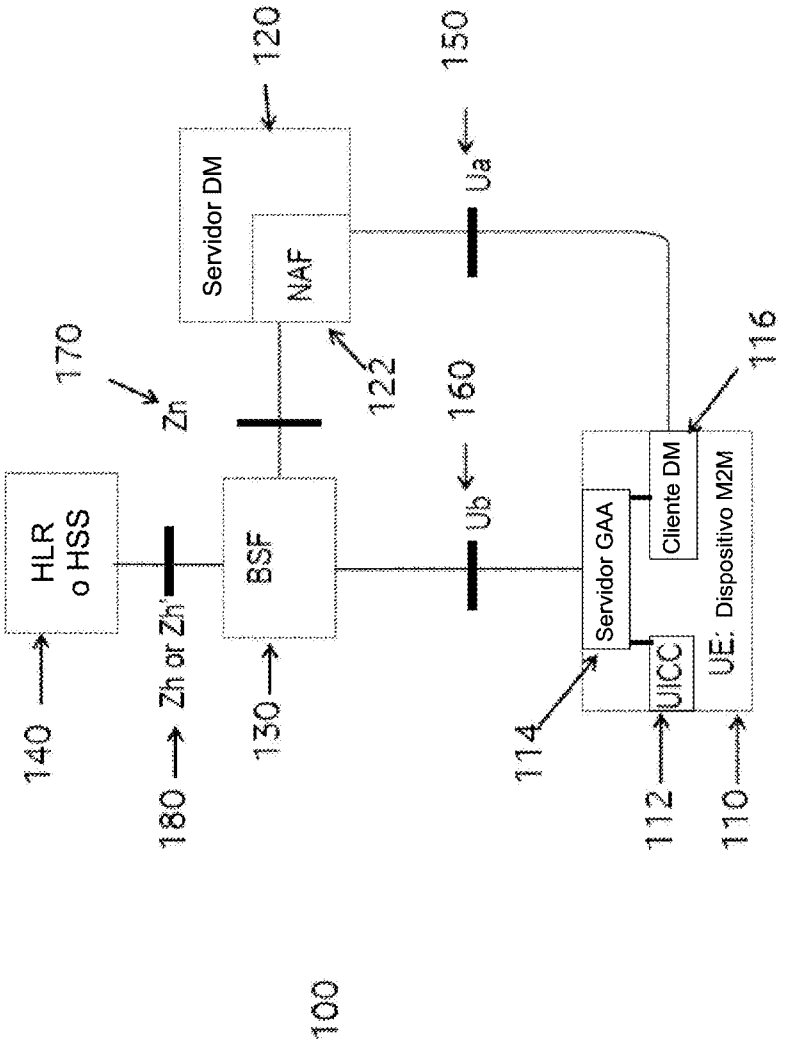

120
150
Servidor DM
NAF
Ua
170
Zn
122
160
116
HLR
o HSS
BSF
Ub
Servidor GAA
Cliente DM
UICC
UE: Dispositivo M2M
140
180
Zh or Zh'
130
114
112
110
100

FIG. 2

Fig. 2

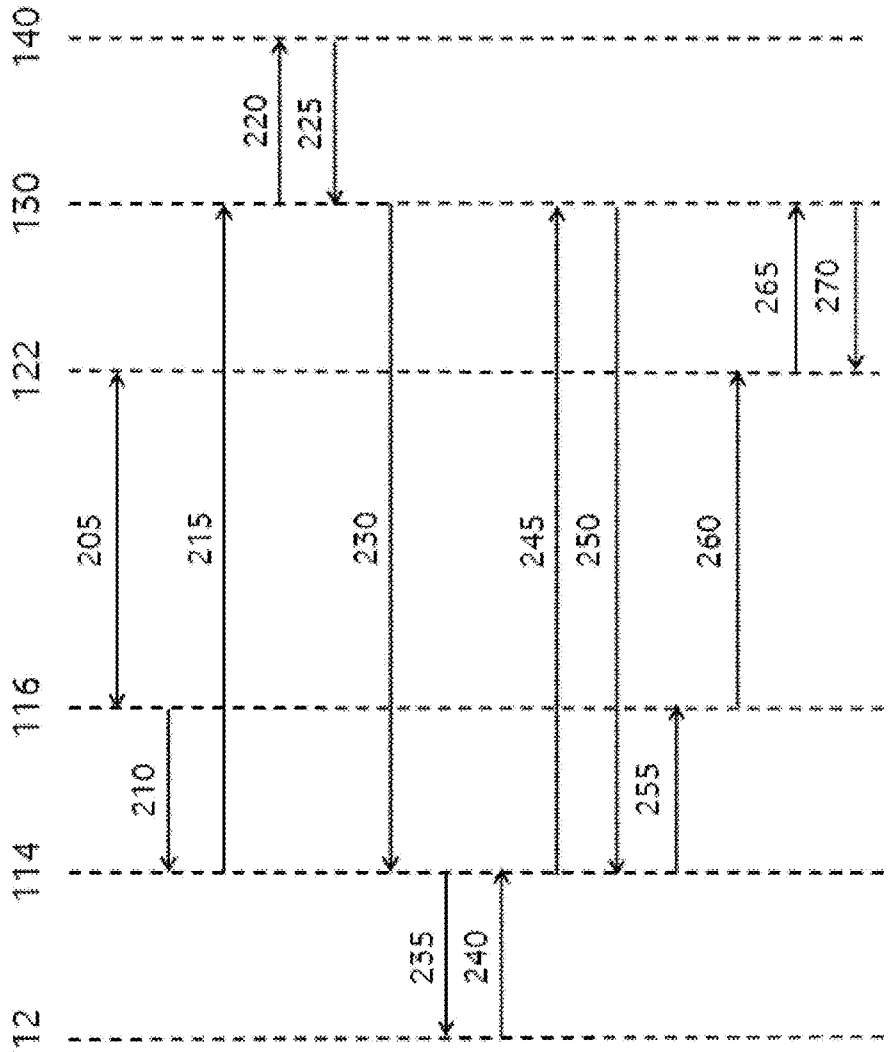

140
130
122
116
114
112
220
225
205
215
230
245
250
260
265
270
210
255
235
240

FIG. 3

Fig. 3

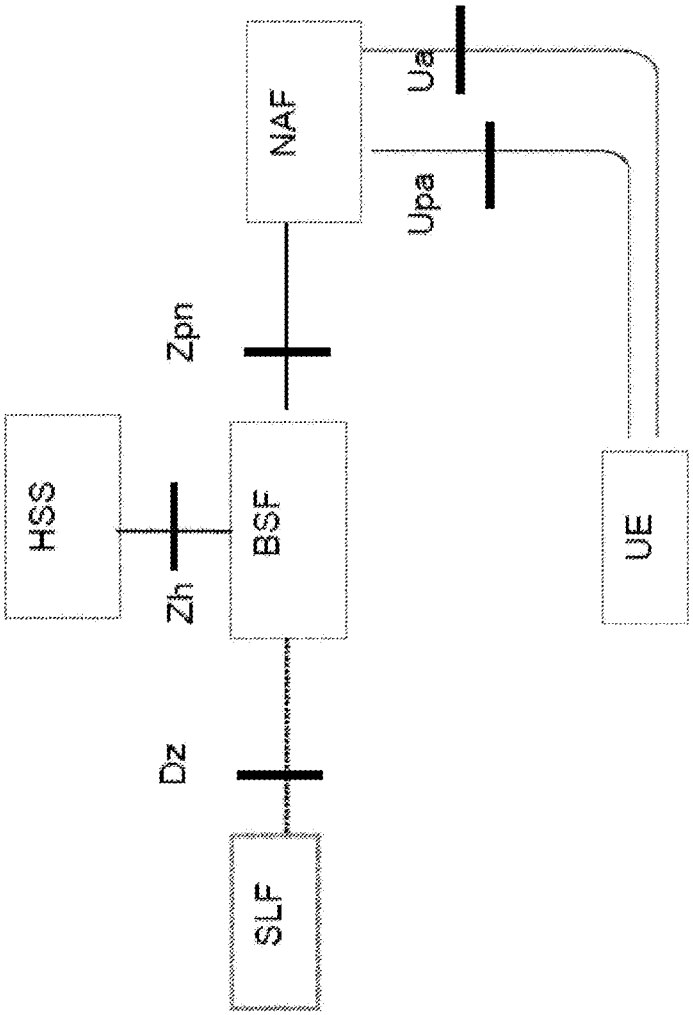


FIG. 4

Fig. 4

Fig. 5

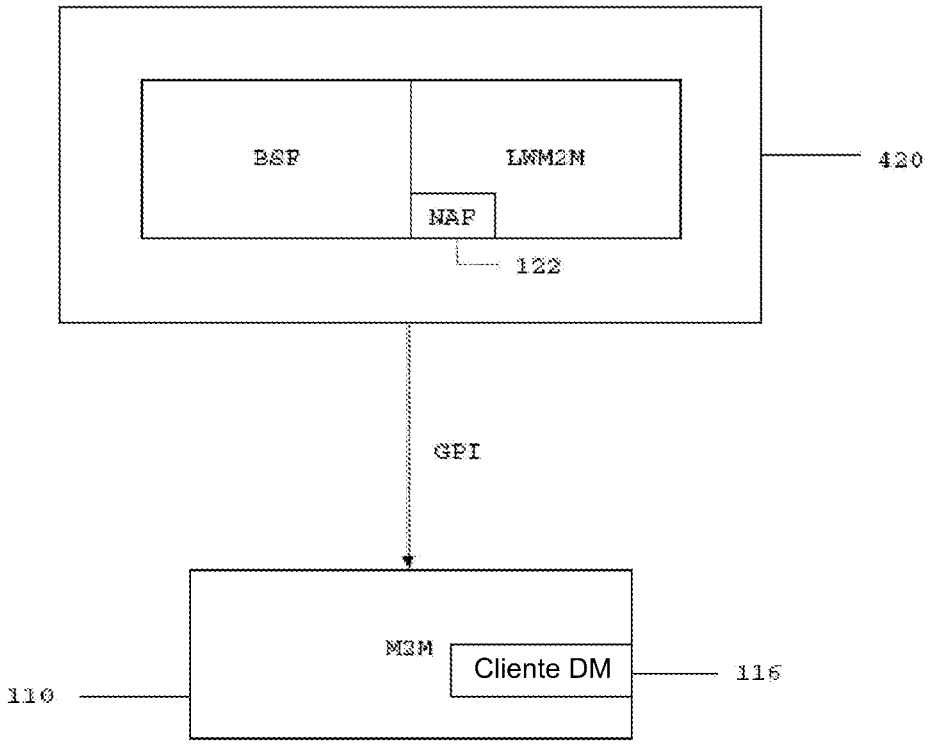


Fig. 6

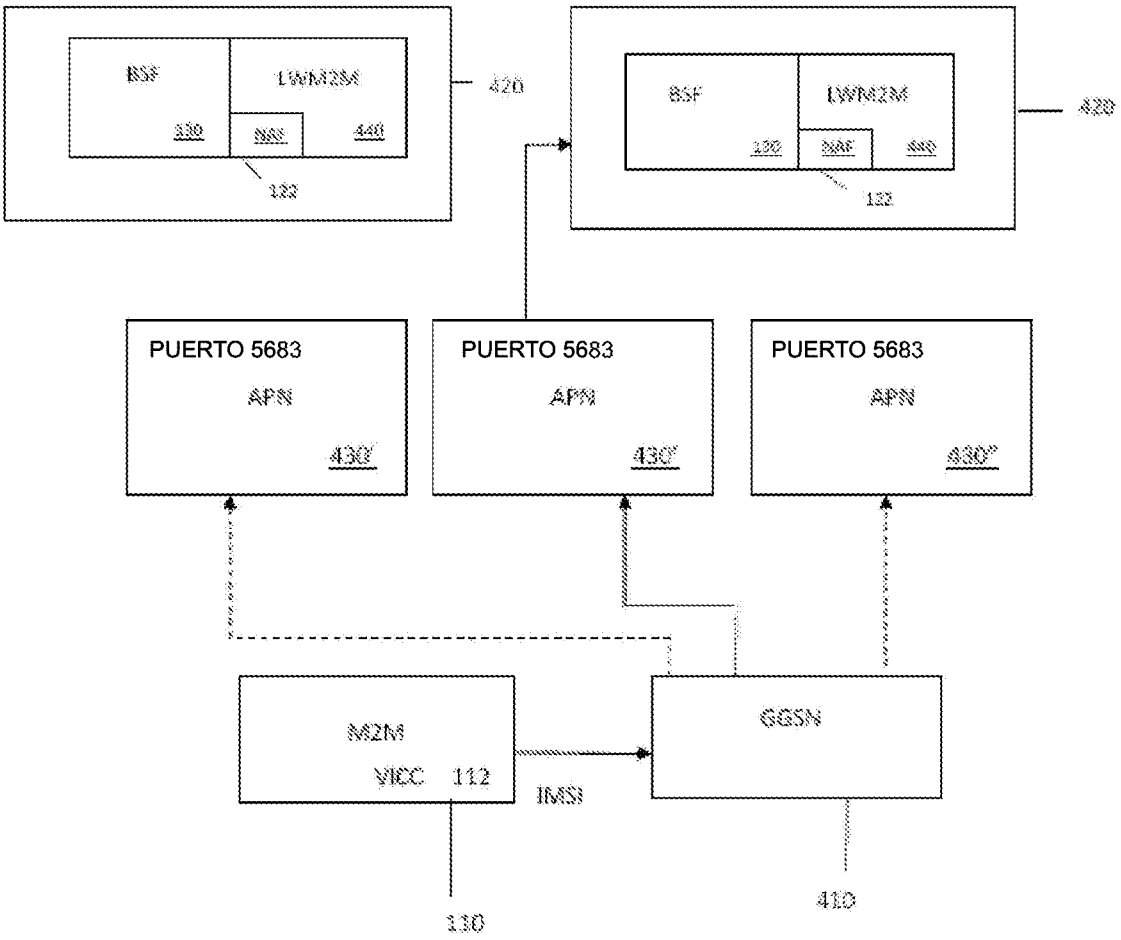

BSF
330
LWM2M
SMS
440
132
420
BSF
330
LWM2M
SMF
440
132
420
PUERTO 5683
APN
430'
PUERTO 5683
APN
430'
PUERTO 5683
APN
430'
M2M
VICC 112
IMSI
GGSN
130
410

Fig. 7

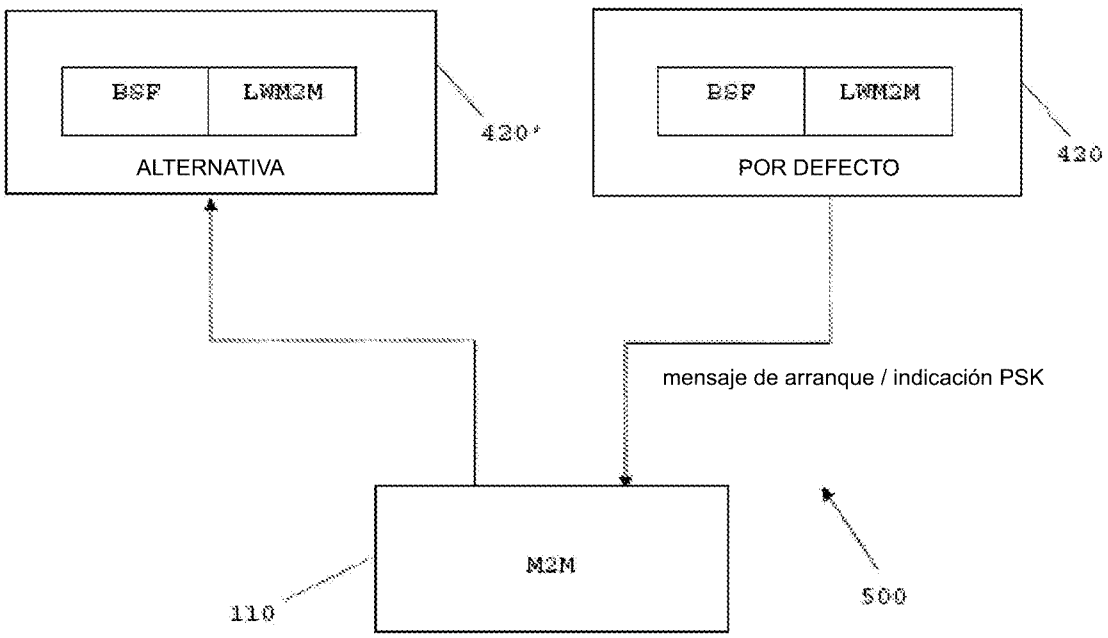

BSF
LWM2M
ALTERNATIVA
420'
BSF
LWM2M
POR DEFECTO
420
mensaje de arranque / indicación PSK
M2M
110
500

Fig. 8

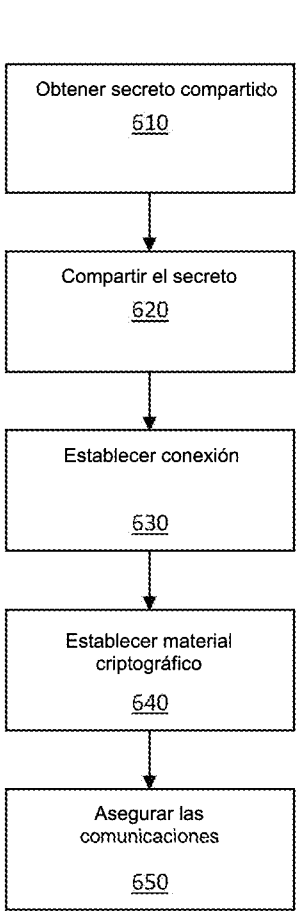
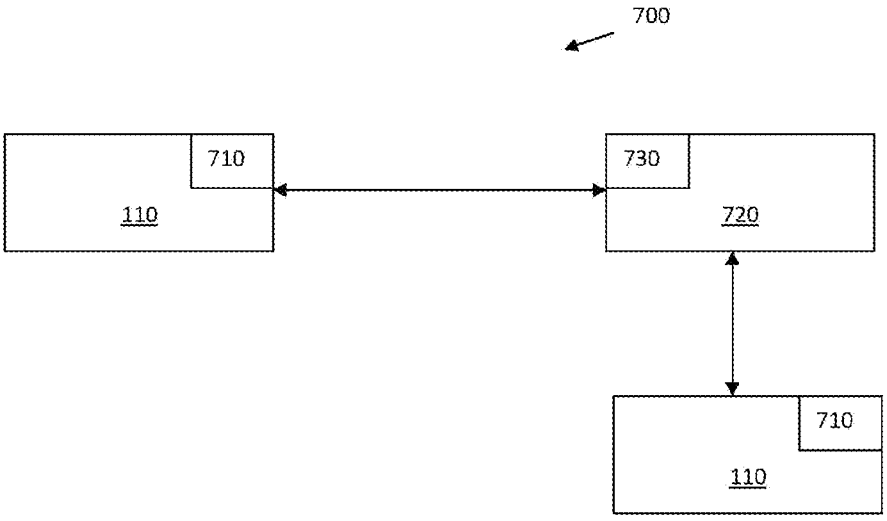

600
Obtener secreto compartido
610
Compartir el secreto
620
Establecer conexión
630
Establecer material criptográfico
640
Asegurar las comunicaciones
650

Fig. 9


700
710
110
730
720
710
110