(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 661 307**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04W 12/04 (2009.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.03.2007 PCT/FI2007/000073**

(87) Fecha y número de publicación internacional: **04.10.2007 WO07110468**

(96) Fecha de presentación y número de la solicitud europea: **26.03.2007 E 07730542 (3)**

(97) Fecha y número de publicación de la concesión europea: **20.12.2017 EP 2005702**

(54) Título: **Autenticación de una aplicación**

(30) Prioridad:

28.03.2006 US 786357 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.03.2018

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

LAKSHMESHWAR, SHREEKANTH;
GINZBOORG, PHILIP;
LAITINEN, PEKKA y
HOLTMANNS, SILKE

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Autenticación de una aplicación

Antecedentes de la invención:

Campo de la invención:

La presente invención se refiere a autenticación. En particular, la presente invención se refiere a métodos novedosos y mejorados, programas informáticos y terminal móvil para autenticar una aplicación de cliente.

Descripción de la técnica relacionada:

El desarrollo actual hacia la informática verdaderamente móvil e interconexión en red móvil ha traído la evolución de diversas tecnologías de acceso, que también proporcionan a los usuarios con el acceso a Internet cuando están fuera de su propia red doméstica. Hasta ahora, el uso de Internet ha sido dominado por comunicaciones de persona a máquina, es decir servicios de información. La evolución hacia las denominadas redes inalámbricas de la tercera generación (3G) trae consigo comunicaciones multimedia móviles, que también cambiarán la manera en la que se utilizan los servicios basados en IP en redes móviles públicas. El Subsistema Multimedia de IP (IMS), como se especifica por el Proyecto Común de Tecnologías Inalámbricas de la 3ª Generación (3GPP), integra comunicaciones de voz móviles con tecnologías de Internet, permitiendo que se utilicen servicios multimedia basados en IP en redes móviles.

Los nuevos terminales móviles aptos para multimedia (teléfonos multimedia) proporcionan una plataforma de desarrollo abierta para desarrolladores de aplicaciones, que permite a los desarrolladores de aplicaciones independientes diseñar nuevos servicios y aplicaciones para el entorno multimedia. Los usuarios pueden descargar, a su vez, las nuevas aplicaciones/servicios a sus terminales móviles y usarlos en los mismos.

Por ejemplo, la especificación técnica 3GPP TS 33.220 desvela la Arquitectura de Arranque Genérica (GBA) que es parte de la Arquitectura de Autenticación Genérica (GAA). Un modelo de red general de la GBA se desvela en la Figura 1. El modelo desvelado en la Figura 1 incluye cuatro entidades diferentes: El equipo de usuario (UE) 14, una Función de Servidor de Arranque (BSF) 12, una Función de Aplicación de Red (NAF) 16 y un Sistema de Abonado Doméstico (HSS) 10. La Figura 1 también desvela las interfaces entre las entidades.

La Figura 2 es un diagrama que ilustra el procedimiento de arranque en la GBA. Cuando el UE 200 desea interactuar con una NAF, y conoce que es necesario el procedimiento de arranque, deberá realizar en primer lugar una autenticación de arranque. Cuando se inicia el arranque, el UE 200 envía (21) una solicitud de HTTP hacia la BSF 202. La BSF 202 recupera (22) el conjunto completo de ajustes de seguridad de usuario de GBA y un Vector de Autenticación (AV, AV = RAND| |AUTN| |XRES| |CK| |IK) a través del punto de referencia Zh desde un HSS 204. A continuación la BSF 202 reenvía RAND y AUTN al UE 200 en 401 el mensaje (23) (sin CK, IK y XRES). Esto es para exigir al UE 200 que se autentique a sí mismo. El UE 200 comprueba (24) AUTN para verificar que el desafío es desde una red autorizada. El UE 200 también calcula CK, IK y RES. Esto dará como resultado las claves de sesión IK y CK tanto en la BSF 202 como en el UE 200. El UE 200 envía (25) otra solicitud de HTTP, que contiene la respuesta Compendio AKA (calculada usando RES), a la BSF 202. La BSF 202 autentica (26) el UE 200 verificando la respuesta de Compendio AKA y genera (27) una clave maestra Ks concatenando CK y IK. Deberá generarse también un valor B-TID. La BSF 202 envía (28) un 200 mensaje OK, que incluye el B-TID, al UE 200 para indicar el éxito de la autenticación. Además, en 200 el mensaje OK, la BSF 202 deberá suministrar el tiempo de vida de la clave Ks. La clave Ks se genera en el UE 200 concatenando CK y IK. Tanto el UE 200 como la BSF 202 deberán usar las K para derivar la clave Ks_NAF. Deberá usarse Ks_NAF para asegurar el punto de referencia Ua (véase la Figura 1).

Ks_NAF se calcula como Ks_NAF = KDF (Ks, parámetros de derivación de clave), donde KDF es una función de derivación de clave adecuada, y los parámetros de derivación de clave comprenden la identidad privada del usuario, la NAF_Id y RAND. La KDF para la GBA se define en 3GPP TS 33.220, Anexo B. La NAF_Id consiste en el nombre de DNS completo de la NAF y el identificador de seguridad de protocolo de Ua. KDF deberá implementarse en el equipo móvil.

Cuando una aplicación en el terminal desea autenticarse en un servidor de aplicación de red, obtiene un secreto compartido específico de NAF Ks_NAF a través de una API ofrecida por una aplicación confiable en el terminal. La aplicación confiable usa los procedimientos de arranque anteriormente descritos con el servidor de Función de Servidor de Arranque (BSF) en la red para derivar el secreto compartido específico de NAF Ks_NAF. La NAF obtiene el secreto compartido para esta aplicación de cliente comunicando con la BSF.

Un proveedor de servicio puede desear evitar que se desarrollen aplicaciones de cliente y sean de propiedad de otros proveedores de servicio y se instalen en un terminal móvil para acceder a su servicio. Para conseguir este objetivo podría, por ejemplo, autenticar una aplicación en el terminal móvil cada vez que intenta acceder al servicio.

Este método, sin embargo, requeriría una asociación de seguridad a largo plazo entre el proveedor de servicio y cada copia desplegada de la aplicación. Mantener estas asociaciones de seguridad a largo plazo puede añadir significativamente costes del proveedor de servicio.

Puesto que la clave específica de NAF, es decir Ks_NAF, es de hecho específica de NAF (es decir servicio), el objetivo puede conseguirse restringiendo al terminal móvil el acceso a Ks_NAF a únicamente aquellas aplicaciones que se confían por el proveedor de servicio de NAF. Esta restricción es posible si el hardware y software de la plataforma del terminal móvil tienen las siguientes propiedades de seguridad: (1) los procesos pueden autenticarse entre sí y (2) un proceso no puede acceder a los datos de otro proceso. El terminal móvil, sin embargo, tiene que configurarse; necesita conocer qué aplicaciones se permite acceder a qué credenciales específicos de NAF (es decir, claves específicas de NAF).

Hay al menos dos opciones para configurar permisos de acceso a credenciales de GBA (es decir, un conjunto de claves específicas de NAF) en el terminal móvil.

En primer lugar, el terminal móvil puede obtener los datos de configuración con permisos para todas las aplicaciones de NAF desde una fuente externa. En este caso se requiere que los datos de configuración provengan de una fuente confiable y estén protegidos en integridad. Los permisos para acceder a credenciales de GBA podrían entregarse al ME junto con otros datos de configuración usando una estructura de gestión de dispositivo (por ejemplo, procedimientos de Gestión de Dispositivo de OMA), que implementan estos requisitos. Los datos de seguridad de configuración podrían basarse en criptografía 1) simétrica, o en 2) asimétrica. Esta opción puede usarse también sin una estructura de gestión de dispositivo externo. Por ejemplo, el terminal móvil puede configurarse antes de que se entregue al usuario final, por ejemplo en la fábrica por el fabricante, o en la tienda por el vendedor del terminal móvil. Después de que el terminal móvil haya alcanzado a su usuario final, los permisos podrían modificarse manualmente: por ejemplo, el terminal móvil solicitará que su propietario configure cada nuevo permiso. Sin embargo, la configuración manual del terminal móvil puede perjudicar la usabilidad de uso de servicio, por lo que es mejor configurar los permisos automáticamente tanto como sea posible. Adicionalmente, una desventaja potencial de esta opción es que la fuente de datos de configuración debe confiarse por todos los proveedores de servicio puesto que define los permisos para todas las aplicaciones de NAF.

En segundo lugar, los derechos de acceso para cada aplicación pueden configurarse en el terminal uno a uno basándose en la comunicación con la fuente externa.

Otro método para configurar los derechos de acceso individualmente para cada aplicación es usar la Infraestructura de Clave Pública (PKI) y aplicaciones firmadas. Normalmente, la firma de una aplicación firmada puede verificarse usando un certificado digital específico de la aplicación. Puede ser que el sistema de PKI usado para certificar y verificar aplicaciones incluya una posibilidad para definir el servicio o servicios, que esta aplicación está permitida a acceder (es decir, a qué credenciales específicos de NAF tiene derechos de acceso la aplicación). Esta información puede codificarse en el mismo certificado de la aplicación, o ser parte de los metadatos de la aplicación. Normalmente, esta información consistiría en identificadores de NAF que identifican cada credencial específica de NAF de manera inequívoca.

La seguridad de configuración con claves simétricas de GBA está basada en el hecho de que la NAF y el terminal móvil comparten la clave Ks_NAF. Dos métodos principales para implementar esta alternativa son: (1) Si una aplicación firmada por Ks_NAF, entonces puede ser confiable para que obtenga acceso a instancias futuras de esos credenciales de NAF, y (2) si una aplicación puede probar una vez que conoce la Ks_NAF del terminal móvil, entonces puede ser confiable que obtenga acceso a instancias futuras de esos credenciales de NAF.

Cuando se instalan aplicaciones de cliente en un terminal móvil, existe una necesidad de establecer una confianza entre esta aplicación y un servidor de GAA_ME (es decir, la aplicación confiable que realiza el procedimiento de arranque con la BSF) instalada en el terminal móvil si esta aplicación desea obtener claves específicas de NAF para que se obtengan desde el servidor de GAA_ME. Sin embargo, hay una manera de firmar la aplicación usando un certificado digital específico de NAF y usar la firma para establecer confianza de la aplicación en el terminal. Por ejemplo esto se está usando en terminales Symbian. Sin embargo, el servidor GAA_ME no tendría conocimiento de cuál de todas las aplicaciones instaladas (confiables), debieran proporcionarse únicamente con claves específicas de NAF.

El problema anteriormente mencionado puede resolverse añadiendo alguna entrada a un certificado que indica que esta aplicación firmada por la aplicación debería proporcionarse con capacidad de cliente GAA (es decir pueden obtenerse credenciales de NAF desde el servidor de GAA_ME a una aplicación de terminal móvil). Esta solución necesita algún mecanismo entre el servidor de GAA_ME y la plataforma (con seguridad de plataforma) para coordinar la confianza. Cuando las aplicaciones cliente se encuentran en el dispositivo de proximidad como un portátil (caso de uso división-terminal), que desea usar el servidor de GAA_ME del teléfono, esta solución se vuelve difícil de implementar.

El documento Gemplus et al: "GAA-based terminal to UICC key establishment", 3GPP draft S3-050378; 21 de junio

de 2005, XP050277712 desvela una solución para establecer un secreto compartido entre un equipo móvil y un UICC que contiene una aplicación de USIM.

El documento Huawei: "GAA based Peripheral Equipment to UICC key establishment", 3GPP draft S3-060015; 31 de enero de 2006, XP050278395 desvela una solución para establecer la clave entre un UICC y un terminal.

Basándose en lo anterior existen varios problemas en las soluciones de la técnica anterior que necesitan resolverse. Por ejemplo, qué aplicaciones en un terminal móvil están permitidas a acceder a qué credenciales de NAF y cómo configurar esto. Adicionalmente, otro problema es cómo autenticar una aplicación a un servidor de GAA_ME en un terminal móvil.

Sumario de la invención:

De acuerdo con un aspecto de la invención, se proporciona un método de autenticación de una aplicación con una aplicación de servidor confiable en un terminal móvil, siendo la aplicación de servidor confiable externa a una tarjeta de circuito integrado universal. El método comprende realizar, con la aplicación de servidor confiable, procedimientos de arranque entre la aplicación de servidor confiable y una función de servidor de arranque; derivar una clave compartida basándose en al menos una clave acordada con el servidor de función de servidor de arranque durante los procedimientos de arranque y un identificador de función de aplicación de red; proporcionar una aplicación con un identificador de transacción de arranque, recibiéndose el identificador de transacción de arranque desde el servidor de función de servidor de arranque durante los procedimientos de arranque; recibir una respuesta desde la aplicación; autenticar la aplicación validando la respuesta con la clave compartida; y marcando, por la aplicación de servidor confiable, la aplicación como confiable cuando la autenticación es satisfactoria.

El aspecto anteriormente mencionado puede implementarse como un programa informático que puede realizarse en un medio legible por ordenador.

De acuerdo con otro aspecto de la invención, se proporciona un terminal móvil para autenticar una aplicación. El terminal móvil comprende una aplicación de servidor confiable que es externa a una tarjeta de circuito integrado universal, la aplicación de servidor confiable está configurada para realizar procedimientos de arranque entre la aplicación de servidor confiable y una función de servidor de arranque; para derivar una clave compartida basándose al menos en una clave material recibida desde el servidor de función de servidor de arranque durante los procedimientos de arranque y un identificador de función de aplicación de red; para proporcionar una aplicación con un identificador de transacción de arranque, recibiéndose el identificador de transacción de arranque desde el servidor de función de servidor de arranque durante los procedimientos de arranque; para recibir una respuesta desde la aplicación; autenticar la aplicación validando la respuesta con la clave compartida; y para marcar la aplicación como confiable cuando la autenticación es satisfactoria.

La presente invención tiene varias ventajas sobre las soluciones de la técnica anterior. Ninguna aplicación de virus o incluso cualquier aplicación de terceros puede solicitar credenciales de GAA desde el servidor de GAA_ME instalado en el equipo móvil a menos que puedan autenticar alguna NAF y derivar un secreto compartido (es decir KS_NAF_instalar) para que se use para registro al servidor de GAA_ME.

Adicionalmente, la invención proporciona una solución para derivar un secreto compartido entre un servidor de GAA_ME y una aplicación en un terminal de proximidad. La solución desvelada en la invención puede usarse para autenticar la aplicación de proximidad hacia el servidor de GAA_ME. Sin embargo, esto puede requerir que exista algún tipo de informática confiable (seguridad de plataforma) en el dispositivo de proximidad también.

Además, la invención proporciona a las operadoras una opción atractiva para distribuir sus aplicaciones. Las operadoras que ya tienen autenticación basada en nombre de usuario-contraseña (o algún otro mecanismo de autenticación), la solución desvelada en la invención hace más fácil moverse hacia el uso de credencial basado en GAA.

Adicionalmente, la invención puede usarse también de modo que dos dispositivos generen una clave compartida de grupo que se usa a continuación para un grupo de comunicación y puede distribuirse adicionalmente a otros usuarios por ejemplo para usarse para establecer túneles seguros entre ellos y para intercambiar certificados para establecer Redes Privadas Virtuales (VPN) entre ellos o simplemente para establecer Seguridad de Capa de Transporte (TLS) entre ellos.

En general, la solución desvelada en la invención puede usarse para instalación de aplicaciones específicas de operadora y crear alguna confianza entre un componente existente y el componente recién instalado.

Breve descripción de los dibujos:

Los dibujos adjuntos, que se incluyen para proporcionar un entendimiento adicional de la invención y constituyen una parte de esta memoria descriptiva, ilustran realizaciones de la invención y junto con la descripción ayudan a explicar

los principios de la invención. En los dibujos:

La **Figura 1** es un diagrama de bloques que ilustra una arquitectura de la técnica anterior de la Arquitectura de Arranque Genérica (GBA),
La **Figura 2** es un diagrama de señalización que ilustra un procedimiento de arranque de la técnica anterior,
La **Figura 3** es un diagrama de bloques que ilustra diversos elementos de acuerdo con una realización de la invención, y
La **Figura 4** es un diagrama de señalización que ilustra una realización para autenticar una aplicación hacia una aplicación de servidor en el equipo móvil de acuerdo con la presente invención.
La **Figura 5** es un diagrama de señalización que ilustra otra realización para autenticar una aplicación hacia una aplicación de servidor en el equipo móvil de acuerdo con la presente invención.

Descripción detallada de las realizaciones preferidas:

Se hará ahora referencia en detalle a las realizaciones de la presente invención, ejemplos de las que se ilustran en los dibujos adjuntos.

La Figura 3 desvela un diagrama de bloques que ilustra diversos elementos que pueden tomar parte en la solución desvelada en la invención disponible. La Figura 3 desvela cinco entidades diferentes: El Equipo Móvil (ME) 300, una Función de Servidor de Arranque (BSF) 302, una Función de Aplicación de Red (NAF) 306, un Sistema de Abonado Doméstico (HSS) 304 y un ordenador 308. El diagrama de bloques de la Figura 3 tiene en cuenta también una situación de división-terminal. En una situación de división-terminal una aplicación local 320 reside por ejemplo en el ordenador 308. La aplicación local está conectada a un servidor de GAA_ME del equipo móvil 314 mediante un módulo de GAA 318 y un módulo de proximidad 312. La conexión real entre el equipo móvil 314 y el ordenador 308 se consigue por ejemplo mediante un enlace de proximidad, por ejemplo Bluetooth. APP_ME 310 es una aplicación (cliente) que está instalada en el equipo móvil 300. En otras palabras, la aplicación puede instalarse en el mismo equipo móvil o en un ordenador 308 que tiene una conexión local al equipo móvil 300.

La arquitectura de GAA proporciona una manera para generar un secreto compartido entre el equipo móvil 300 y la NAF 306. Este secreto se usa cada vez que el equipo móvil 300 desea autenticarse en la NAF 306. Las aplicaciones en el equipo móvil 300 necesitan credenciales de USIM (o ISIM o SIM) para llevar a cabo arranque de GAA para generar claves específicas de NAF. La capacidad para obtener credenciales de USIM desde el USIM preferentemente no debería ponerse a disposición de todas las aplicaciones en el equipo móvil 300 debido a una amenaza de seguridad. Por lo tanto, un servidor de GAA_ME confiable 314 puede instalarse en el equipo móvil 300 durante la producción o más tarde, que tiene la capacidad para obtener credenciales de USIM del USIM y por lo tanto la capacidad para hacer el arranque para generar credenciales de NAF. Entonces, una aplicación cliente (APP_ME) usaría los servicios del servidor de GAA_ME 314 para obtener los credenciales específicos de NAF. Tal aplicación de cliente de GAA_ME está preparada y empaquetada por el proveedor de NAF. Tal aplicación se firma usando una firma digital que entiende la plataforma (symbian, xp, Linux, java, etc.). Después de la instalación tal aplicación se registra en el servidor de GAA_ME 314 durante la primera vez de su ejecución.

El equipo móvil 300 y la función de aplicación de red 306 pueden incluir una memoria o memorias (no desveladas en la Figura 3) que pueden incluir también un programa informático (o porción del mismo), que cuando se ejecuta en una unidad de procesamiento de datos realiza al menos algunas de las etapas de la invención. La unidad de procesamiento de datos puede incluir también memoria o una memoria puede estar asociada con la misma que puede incluir el programa informático (o porción del mismo) que cuando se ejecuta en la unidad de procesamiento de datos realiza al menos algunas de las etapas de la invención.

La Figura 4 es un diagrama de señalización que ilustra una realización para registrar y autenticar una aplicación a una aplicación de servidor en el equipo móvil de acuerdo con la presente invención. La Figura 4 desvela tres entidades diferentes: un servidor de Función de Servidor de Arranque (BSF) 400, un servidor de Función de Aplicación de Red (NAF) 402 y el Equipo Móvil (ME) 404. El equipo móvil 404 incluye una aplicación de cliente APP_ME 406 y una aplicación de servidor GAA_ME 408 ya desveladas en la Figura 3. En otra realización, la aplicación de cliente APP_ME puede residir fuera del equipo móvil 404, es decir, por ejemplo en un dispositivo externo conectado al equipo móvil 404.

En la realización de la Figura 4, la APP_ME 406 envía una solicitud de registro (410) al servidor de GAA_ME 408. La solicitud indica al servidor de GAA_ME 408 que la APP_ME desea autenticarse a sí misma en el servidor GAA_ME 408. La solicitud puede contener también un identificador de NAF y/o un identificador de instancia de aplicación. El proveedor de aplicación puede tener pre-programada la aplicación o, de alguna manera, estar configurado para tener el identificador de NAF y el identificador de instancia de aplicación en su lugar.

El servidor de GAA_ME 408 lleva a cabo (412) un protocolo de arranque de 3GPP con la BSF 400. El protocolo de arranque se desvela en más detalle por ejemplo en la especificación técnica del 3GPP 3GPP TS 33.220 V7.2.0 (12-2005). Durante el arranque el servidor de GAA_ME 408 recibe al menos un BTID (Identificador de Transacción de Arranque) y el tiempo de vida de la clave desde la BSF 400 y pasa (414) al menos el BTID de vuelta a la APP_ME

406. Puesto que el servidor de GAA_ME 408 puede derivar las K materiales y conoce el identificador de NAF, puede derivar la clave Ks_NAF que es un secreto compartido entre el servidor de GAA_ME 408 y la NAF 402. El servidor de GAA_ME 408 derivará a continuación (422) una clave de instalación KS_NAF_instalar usando KS_NAF y opcionalmente el identificador de instancia de aplicación anteriormente mencionado usando cualquier método apropiado.

Después de recibir el BTID desde el servidor de GAA_ME 408, la APP_ME 406 abre un enlace de comunicación con la NAF 402. El enlace de comunicación puede asegurarse para mitigar posibles ataques de hombre en el medio usando por ejemplo la Capa de Conexión Segura (SSL) o cualquier otro método apropiado.

Después de eso la APP_ME 406 se autentica (416) a sí misma en la NAF 402 usando un procedimiento de autenticación apropiado. Existen varios métodos de autenticación aplicables en la técnica anterior que pueden usarse. El procedimiento de autenticación puede incluir uno de los siguientes:

- Contraseña de un solo uso pre-grabada en la aplicación. En este caso se prefiere que el código de la aplicación esté ofuscado de modo que sea muy difícil recuperar la contraseña simplemente examinando el código.
- Nombre de usuario y contraseña obtenidos fuera de banda (como publicación o visitas a una tienda).
- Registrar en la NAF en línea para obtener los credenciales.

Adicionalmente, el método de autenticación y aseguración del canal puede ser específico de NAF. La clave compartida TLS puede usarse también en caso de secretos compartidos. También, los métodos de autenticación HTTP-DIGEST son bien usados para autenticación.

Una vez que se ha autenticado la APP_ME 406 a la NAF 402, la NAF 402 capturará (418) la clave específica de NAF KS_NAF desde la BSF 400 usando el BTID y derivará (420) KS_NAF_instalar (similar a la etapa 422). A continuación transfiere (424) KS_NAF_instalar a la APP_ME 406. Esa transferencia debería ser preferentemente confidencial.

Ahora, la APP_ME 406 puede autenticarse (426) a sí misma al GAA_ME_servidor 408 usando KS_NAF_instalar como un secreto compartido. Si la autenticación es satisfactoria el servidor de GAA_ME 408 puede añadir (428) la aplicación en su lista de aplicaciones confiables dependiendo de su configuración local. Por lo tanto, la etapa 428 puede también ser una etapa opcional. Si la aplicación está en la lista de aplicaciones confiables, siempre que en el futuro la APP_ME 406 realice una solicitud para claves de NAF, el servidor de GAA_ME 408 arranca y proporciona las claves de NAF sin ninguna autorización adicional de la NAF 402.

En la realización desvelada en la Figura 4, los dos recuadros de derivación de clave de instalación (420, 422) se colocan en el mismo nivel. Sin embargo, cada uno puede moverse hacia arriba o abajo dependiendo del requisito. La derivación de la clave de instalación puede hacerse usando por ejemplo función de troceo usando KS_(ext)_NAF y el identificador de instancia de aplicación o simplemente usar la misma KS_(ext)_NAF como KS_NAF_instalar.

El secreto compartido usado para autenticar inicialmente la APP_ME 406 y la NAF 402 puede también ser una contraseña de un solo uso. La contraseña puede borrarse en la NAF 402 una vez que el terminal establece confianza con el servidor de GAA_ME del cliente 408. El secreto compartido puede derivarse también basándose en alguna característica del terminal móvil. Adicionalmente, el mismo protocolo de autenticación entre la APP_ME 406 y la NAF 402 puede ser cualquiera de los protocolos de autenticación bien conocidos. Una vez que se ha realizado la autenticación, el método de aseguración de la comunicación entre AP_ME 406 y NAF 402 puede ser uno de los métodos bien conocidos. Si se usa un secreto compartido (por ejemplo nombre de usuario y contraseña), el protocolo TLS de clave compartida es una alternativa.

En una realización de la invención, cuando el servidor de GAA_ME 408 ha autenticado satisfactoriamente la APP_ME 406, usando un cierto id de NAF, el servidor de GAA_ME 408 puede conceder el acceso de APP_ME únicamente a las instancias futuras de la clave Ks_NAF que pertenece al mismo id de NAF, y otras claves específicas de NAF no serían accesibles. En otra realización de la invención, se concede un acceso total a la APP_ME 406, es decir, puede obtener las claves KS_NAF de cualquier NAF.

Adicionalmente, en una realización de la invención, durante el procedimiento, pueden usarse múltiples claves Ks_NAF para conceder acceso a múltiples claves, es decir, la NAF 402 captura múltiples claves Ks_NAF desde la BSF 400 (con la condición de que esté autorizada a hacer esto), y la NAF 402 deriva múltiples claves Ks_NAF_instalar y las envía a la APP_ME 406. La APP_ME 406 puede a continuación registrarlas con el servidor de GAA_ME 408. De esta manera la APP_ME 406 obtendría acceso a más de una clave específica de NAF.

La Figura 5 es un diagrama de señalización que ilustra otra realización para registrar y autorizar una aplicación a una aplicación de servidor en el equipo móvil de acuerdo con la presente invención. La Figura 5 desvela tres entidades diferentes: un servidor de Función de Servidor de Arranque (BSF) 500, un servidor de Función de Aplicación de Red (NAF) 502 y el Equipo Móvil (ME) 504. El equipo móvil 504 incluye una aplicación de cliente APP_ME 506 y una aplicación de servidor GAA_ME 508 ya desveladas en la Figura 3. En otra realización, la aplicación de cliente

APP_ME puede residir fuera del equipo móvil 504, es decir, por ejemplo en un dispositivo externo conectado al equipo móvil 504.

En la realización de la Figura 5, la APP_ME 506 envía una solicitud de registro (510) al servidor de GAA_ME 508. La solicitud indica al servidor de GAA_ME 508 que la APP_ME desea autorizarse a sí misma al servidor de GAA_ME 508. La solicitud puede contener también un identificador de NAF y/o un identificador de instancia de aplicación. El proveedor de aplicación puede tener pre-programada la aplicación o, de alguna manera, estar configurado para tener el identificador de NAF y el identificador de instancia de aplicación en su lugar.

El servidor de GAA_ME 508 lleva a cabo (512) un protocolo de arranque de 3GPP con la BSF 500. El protocolo de arranque se desvela en más detalle por ejemplo en la especificación técnica del 3GPP 3GPP TS 33.220 V7.2.0 (12-2005). Durante el arranque el servidor de GAA_ME 508 recibe al menos un BTID (Identificador de Transacción de Arranque) y el tiempo de vida de clave desde la BSF 500. Puesto que el servidor de GAA_ME 508 puede derivar la clave K y conoce el identificador de NAF, puede derivar la clave Ks_NAF (514) que es un secreto compartido entre el servidor de GAA_ME 508 y la NAF 502. El servidor de GAA_ME 508 generará (514) también un desafío aleatorio para la APP_ME (506). Después de esto el servidor de GAA_ME 508 pasa (514) al menos el BTID y el desafío a la APP_ME 506.

Después de recibir el BTID y el desafío desde el servidor de GAA_ME 508, la APP_ME 506 abre un enlace de comunicación con la NAF 502, y pasa (518) el B-TID, y el desafío a la NAF 502. El enlace de comunicación puede asegurarse para mitigar posibles ataques de hombre en el medio.

La NAF 502 captura (520) la clave específica de NAF KS_NAF desde la BSF 400 usando el BTID y deriva (522) una respuesta al desafío usando Ks_NAF. La respuesta puede calcularse por ejemplo usando una función de troceo de un sentido o código de autenticación de mensaje de troceo con clave (HMAC) donde los parámetros de entrada incluyen al menos la Ks_NAF y el desafío. La NAF 502 puede firmar también datos con la Ks_NAF. Los datos pueden incluir una o más funciones de troceo de aplicaciones que la NAF 502 autoriza a tener acceso a las claves específicas de NAF (Ks_NAF). Una de estas funciones de troceo puede ser la función de troceo de la aplicación de APP_ME (506) que se ha instalado en el ME (504) anteriormente. Debería observarse que la función de troceo de la aplicación es simplemente una posibilidad. Cualquier otra pieza de información, es decir, una caracterización adecuada de la aplicación puede usarse en lugar de una función de troceo. Por ejemplo, si la aplicación reside en otro dispositivo que está conectado al terminal del usuario a través de red local, tal como WLAN o Bluetooth, entonces la caracterización de la aplicación puede ser la dirección de red del dispositivo. También, una posible caracterización de una aplicación en un dispositivo externo puede ser el número de serie de ese dispositivo. Además, una posible caracterización sería una clave pública de firma de contenido. Adicionalmente, en una realización de la invención, la solicitud (518) a la NAF 502 puede incluir alguna caracterización de la plataforma (por ejemplo "dispositivo Nokia que ejecuta Serie 60 v3.1") que entonces ayuda a la NAF 502 a enviar de vuelta la caracterización aceptable correcta de la aplicación. Entonces la NAF 502 (524) transfiere la respuesta y posiblemente los datos firmados a la APP_ME 506.

Los datos firmados hacen referencia por ejemplo a algún dato adicional que la NAF 502 añade al mensaje, que se firma usando la Ks_NAF. De esta manera el servidor de GAA_ME puede verificar la firma de estos datos adicionales y estar seguro de que provienen de una fuente confiable, que conoce la Ks_NAF.

Ahora, la APP_ME 506 puede autorizarse (526) a sí misma al GAA_ME_servidor 508 usando la respuesta y los datos firmados. Si la autorización es satisfactoria, es decir, la respuesta y la firma de los datos firmados son correctas, el servidor de GAA_ME 508 continúa con el procedimiento de autorización, y concede acceso a la APP_ME 506 a la Ks_NAF. Adicionalmente, el servidor de GAA_ME 508 puede calcular también la función de troceo de la APP_ME 506, y comprobar si esta función de troceo está en los datos firmados. Si al menos una de las comprobaciones anteriores es satisfactoria el servidor de GAA_ME 508 puede añadir (528) la aplicación en su lista confiable dependiendo de su configuración local. Si la aplicación está en la lista confiable, cada vez que en el futuro la APP_M E 506 realice una solicitud para claves de NAF, el servidor de GAA_ME 508 arranca y proporciona las claves de NAF sin ninguna autorización adicional de la NAF.

Añadiendo posiblemente la aplicación en su lista confiable proporciona la posibilidad de tener "concesiones de un solo uso" y "concesiones totales". En el primer caso la APP_ME tendría siempre que conseguir la autorización adicional (respuesta o datos firmados o ambos) para cada solicitud para Ks_NAF, o en el segundo caso la APP_ME obtendría una concesión permanente y no tendría que obtener la autorización adicional en las futuras solicitudes para Ks_NAF.

Finalmente, si las verificaciones realizadas anteriormente han sido satisfactorias, el servidor de GAA_ME 508 (530) indica a la APP_ME que el procedimiento fue satisfactorio, y posiblemente incluye Ks_NAF a este mensaje.

En una realización de la invención, cuando el servidor de GAA_ME 508 ha autenticado satisfactoriamente la APP_ME 506, el servidor de GAA_ME 408 puede conceder acceso únicamente a la clave específica de NAF específica Ks_NAF que se usó durante el procedimiento, y otras claves específicas de NAF no serían accesibles.

Especialmente, este puede ser el caso si los datos firmados no se enviaran desde la NAF 502 al servidor de GAA_ME 508 a través de APP_ME 506. En otra realización de la invención, se concede un acceso total a la APP_ME 506, es decir, puede obtener todas las claves KS_NAF posibles.

En otra realización de la invención, la KS_(ext)_NAF se usa como una clave de grupo, para asegurar un grupo de comunicación y que pueda compartirse con otros dispositivos que pueden no tener ninguna forma de generación de clave de GBA o capacidad de solicitud en absoluto. Esta realización puede usarse para asegurar un enlace de comunicación, por ejemplo en un entorno virtual con muchos dispositivos de baja capacidad o para establecer una VPN (Red Privada Virtual) personal.

Adicionalmente, en una realización de la invención, puede enviarse NAF_ID desde la APP_ME 506 al servidor de GAA_ME 508 en la etapa 510 como se ha descrito anteriormente o en la etapa 526.

Adicionalmente, en una realización de la invención, durante el procedimiento, pueden usarse múltiples claves Ks_NAF para conceder acceso a múltiples claves, es decir, la NAF 502 captura múltiples claves Ks_NAF desde la BSF 500 (con la condición de que esté autorizado a hacer esto), y la NAF 502 calcula múltiples respuestas al desafío usando estas claves Ks_NAF, y también firma opcionalmente los datos usando todas o el subconjunto de las claves Ks_NAF, y las envían a la APP_ME 506. La APP_ME 506 puede a continuación registrarlas con el servidor de GAA_ME 508. De esta manera la APP_ME 506 obtendría acceso a más de una clave específica de NAF.

Adicionalmente, este método puede aplicarse en muchos otros casos de uso, en los que el equipo terminal está configurado para confiar en un proveedor de servicio (por ejemplo un fabricante de equipo, o por una operadora de red) y así el equipo terminal y el proveedor de servicio pueden tener, o pueden acordar, una clave compartida. Hemos descrito en detalle cómo, si una nueva aplicación puede probar al terminal que se confía por un dicho proveedor de servicio entonces puede marcarse "confiable" e instalarse en el terminal del usuario. Esa prueba está basada en conocimiento de la clave compartida entre el terminal y el proveedor de servicio.

Por ejemplo, en lugar de la aplicación a instalarse en el terminal, podría ser un dispositivo periférico u otro terminal en una red de proximidad (por ejemplo Bluetooth, o red WLAN) que desea conectar al terminal del usuario. El procedimiento de establecimiento de confianza es el mismo también en estos casos.

GBA de 3GPP es una de las maneras para derivar la clave compartida y establecer confianza entre el terminal y el proveedor de servicio. Pueden concebirse otras maneras también. Por ejemplo, con infraestructura de clave pública (PKI) en su lugar, ambas partes intercambiarían certificados de sus claves públicas, verificando la firma uno del otro y continuando para derivar una clave compartida. O, como otro ejemplo, puede preinstalarse una clave compartida a largo plazo en el terminal por el operador de red o el fabricante de terminal.

Es evidente para un experto en la materia que con el avance de la tecnología, la idea básica de la invención puede implementarse de diversas maneras. La invención y sus realizaciones por lo tanto no están limitadas a los ejemplos anteriormente descritos, en su lugar pueden variar dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Un método de autenticación de una aplicación (310, 320) con una aplicación de servidor confiable (314) en un terminal móvil (300), siendo la aplicación de servidor confiable (314) externa a una tarjeta de circuito integrado universal (316), comprendiendo el método:

realizar, con la aplicación de servidor confiable (314), procedimientos de arranque entre la aplicación de servidor confiable (314) y una función de servidor de arranque (302);
derivar, por parte de la aplicación de servidor confiable (314), una clave compartida basándose al menos en una clave recibida desde el servidor de función de servidor de arranque (302) durante los procedimientos de arranque y un identificador de función de aplicación de red;
proporcionar, por parte de la aplicación de servidor confiable (314), la aplicación (310, 320) con un identificador de transacción de arranque, recibiéndose el identificador de transacción de arranque desde el servidor de función de servidor de arranque (302) durante los procedimientos de arranque;
recibir, por parte de la aplicación de servidor confiable (314), una respuesta desde la aplicación (310, 320);
autenticar, por parte de la aplicación de cliente de servidor confiable (314), la aplicación (310, 320) validando la respuesta con la clave compartida; y marcando, por parte de la aplicación de servidor confiable (314), la aplicación (310, 320) como confiable cuando la autenticación es satisfactoria.

2. El método de acuerdo con la reivindicación 1, en el que la autenticación de la aplicación (310, 320) comprende:

autenticar la aplicación (310, 320) comparando la clave compartida con la respuesta.

3. El método de acuerdo con la reivindicación 1, que comprende adicionalmente:

generar un desafío;
proporcionar la aplicación (310, 320) con el desafío; y
en el que la etapa de autenticación comprende autenticar la aplicación (310, 320) validando la respuesta con el desafío y la clave compartida.

4. El método de acuerdo con la reivindicación 3, que comprende adicionalmente:

recibir datos firmados con la respuesta; y en el que la etapa de autenticación comprende adicionalmente verificar los datos firmados con la clave compartida.

5. El método de acuerdo con la reivindicación 1, que comprende adicionalmente:

recibir una solicitud de registro desde la aplicación (310, 320), comprendiendo la solicitud al menos uno del identificador de función de aplicación de red y un identificador de instancia de aplicación antes de proporcionar la aplicación (310, 320) con el identificador de transacción de arranque.

6. El método de acuerdo con la reivindicación 1, que comprende adicionalmente:

recibir una solicitud de registro desde la aplicación (310, 320), antes de proporcionar la aplicación (310, 320) con el identificador de transacción de arranque.

7. El método de acuerdo con la reivindicación 6, en el que la solicitud de registro comprende un identificador de instancia de aplicación.

8. El método de acuerdo con las reivindicaciones 5 o 7, en el que la derivación de la clave compartida comprende:

derivar la clave compartida basándose en la clave recibida desde el servidor de función de servidor de arranque (302) durante los procedimientos de arranque, el identificador de función de aplicación de red y el identificador de instancia de aplicación.

9. El método de acuerdo con la reivindicación 1, que comprende adicionalmente:

proporcionar la aplicación (310, 320) con la clave compartida.

10. El método de acuerdo con la reivindicación 1, que comprende adicionalmente:

recibir desde la aplicación (310, 320) una solicitud para una clave de función de aplicación de red y enviar a la aplicación la clave de función de aplicación de red en respuesta a la solicitud.

11. Un programa informático de autenticación de una aplicación, comprendiendo el programa informático código adaptado para realizar el método de cualquiera de las reivindicaciones 1 - 10, cuando se ejecuta en un procesador.

12. El programa informático de acuerdo con la reivindicación 11, en donde el programa informático se realiza en un medio legible por ordenador.

13. Un terminal móvil (300) para autenticar una aplicación (310, 320), que comprende:

una aplicación de servidor confiable (314) en el terminal móvil (300), siendo la aplicación de servidor confiable (314) externa a una tarjeta de circuito integrado universal (316), estando la aplicación de servidor confiable (314) configurada para realizar procedimientos de arranque entre la aplicación de servidor confiable (314) y una función de servidor de arranque (302), para derivar una clave compartida basándose al menos en una clave recibida desde el servidor de función de servidor de arranque (302) durante los procedimientos de arranque y un identificador de función de aplicación de red, para proporcionar la aplicación (310, 320) con un identificador de transacción de arranque, recibiéndose el identificador de transacción de arranque desde el servidor de función de servidor de arranque (302) durante los procedimientos de arranque, para recibir una respuesta desde la aplicación (310, 320), para autenticar la aplicación (310, 320) validando la respuesta con la clave compartida y para marcar la aplicación (310, 320) como confiable cuando la autenticación es satisfactoria.

14. El terminal móvil (300) de acuerdo con la reivindicación 13, en el que la aplicación de servidor confiable (314) está configurada para autenticar la aplicación (310, 320) comparando la clave compartida con la respuesta.

15. El terminal móvil (300) de acuerdo con la reivindicación 13, en el que la aplicación de servidor confiable (314) está configurada para generar un desafío, para proporcionar la aplicación (310, 320) con el desafío y para validar la respuesta con el desafío y la clave compartida.

16. El terminal móvil (300) de acuerdo con la reivindicación 15, en el que la aplicación de servidor confiable (314) está configurada para recibir datos firmados con la respuesta y la etapa de autenticación comprende adicionalmente verificar los datos firmados con la clave compartida.

17. El terminal móvil (300) de acuerdo con la reivindicación 13, en el que la aplicación de servidor confiable (314) está configurada para recibir una solicitud de registro desde la aplicación (310, 320), comprendiendo la solicitud al menos uno del identificador de función de aplicación de red y un identificador de instancia de aplicación antes de proporcionar la aplicación (310, 320) con el identificador de transacción de arranque.

18. El terminal móvil (300) de acuerdo con la reivindicación 15, en el que la aplicación de servidor confiable (314) está configurada para recibir una solicitud de registro desde la aplicación (310, 320), antes de proporcionar la aplicación (310, 320) con el identificador de transacción de arranque.

19. El terminal móvil (300) de acuerdo con la reivindicación 18, en el que la solicitud de registro comprende un identificador de instancia de aplicación.

20. El terminal móvil (300) de acuerdo con las reivindicaciones 17 o 19, en el que la aplicación de servidor confiable (314) está configurada para derivar la clave compartida basándose en la clave recibida desde el servidor de función de servidor de arranque (302) durante los procedimientos de arranque, el identificador de función de aplicación de red y el identificador de instancia de aplicación.

21. El terminal móvil (300) de acuerdo con la reivindicación 13, en el que la aplicación de servidor confiable (314) está configurada para proporcionar la aplicación (310, 320) con la clave compartida.

22. El terminal móvil (300) de acuerdo con la reivindicación 13, en el que la aplicación de servidor confiable (314) está configurada para recibir desde la aplicación (310, 320) una solicitud para una clave de función de aplicación de red y para enviar a la aplicación (310, 320) la clave de función de aplicación de red en respuesta a la solicitud.

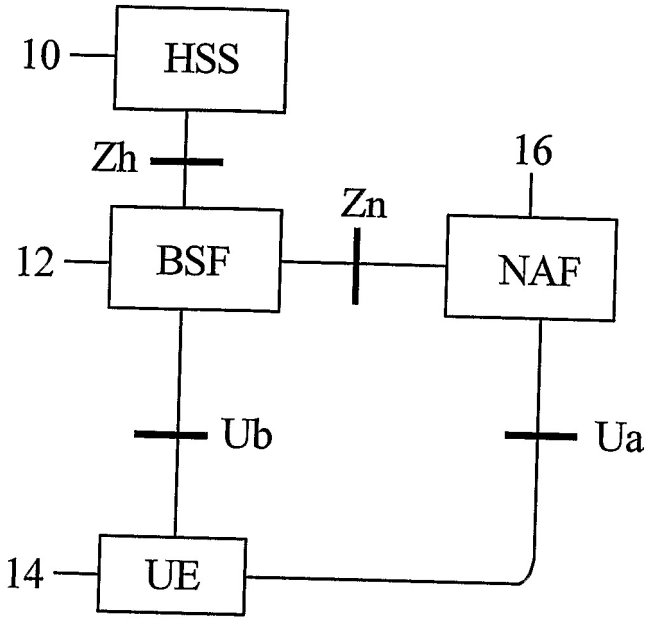

Fig. 1 (TÉCNICA ANTERIOR)

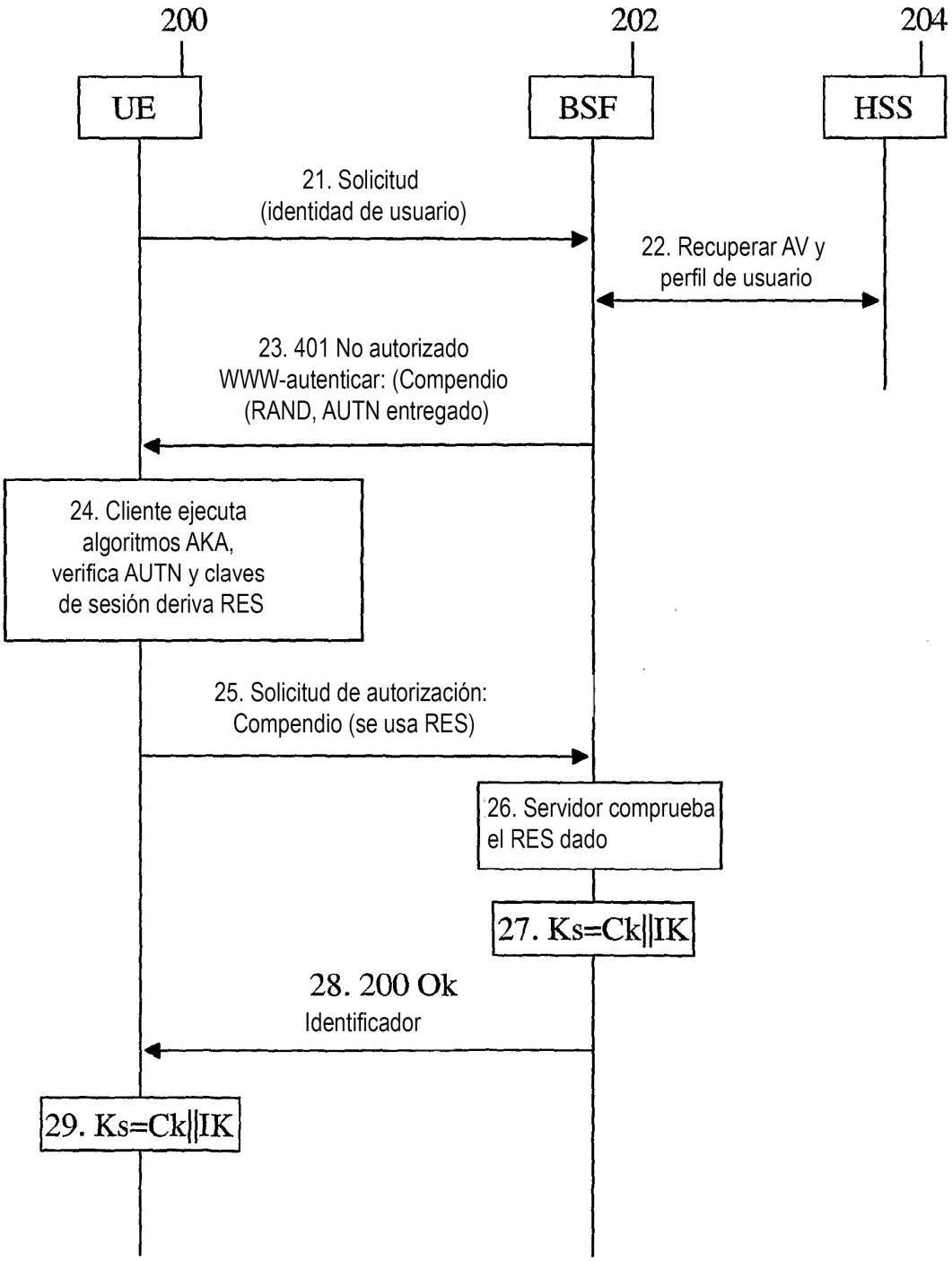

Fig. 2 (TÉCNICA ANTERIOR)

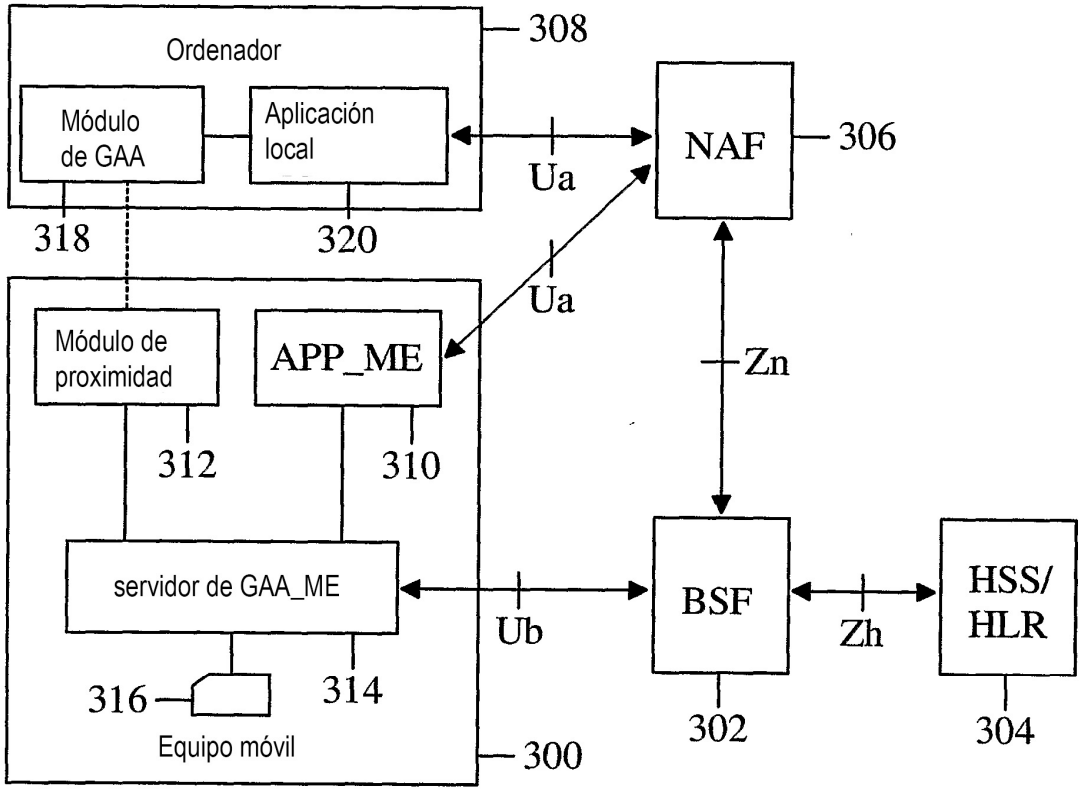
Ordenador
308
Módulo de GAA
Aplicación local
Ua
NAF
306
318
320
Ua
Módulo de proximidad
APP_ME
Zn
312
310
servidor de GAA_ME
Ub
BSF
Zh
HSS/ HLR
316
314
302
304
Equipo móvil
300

Fig. 3

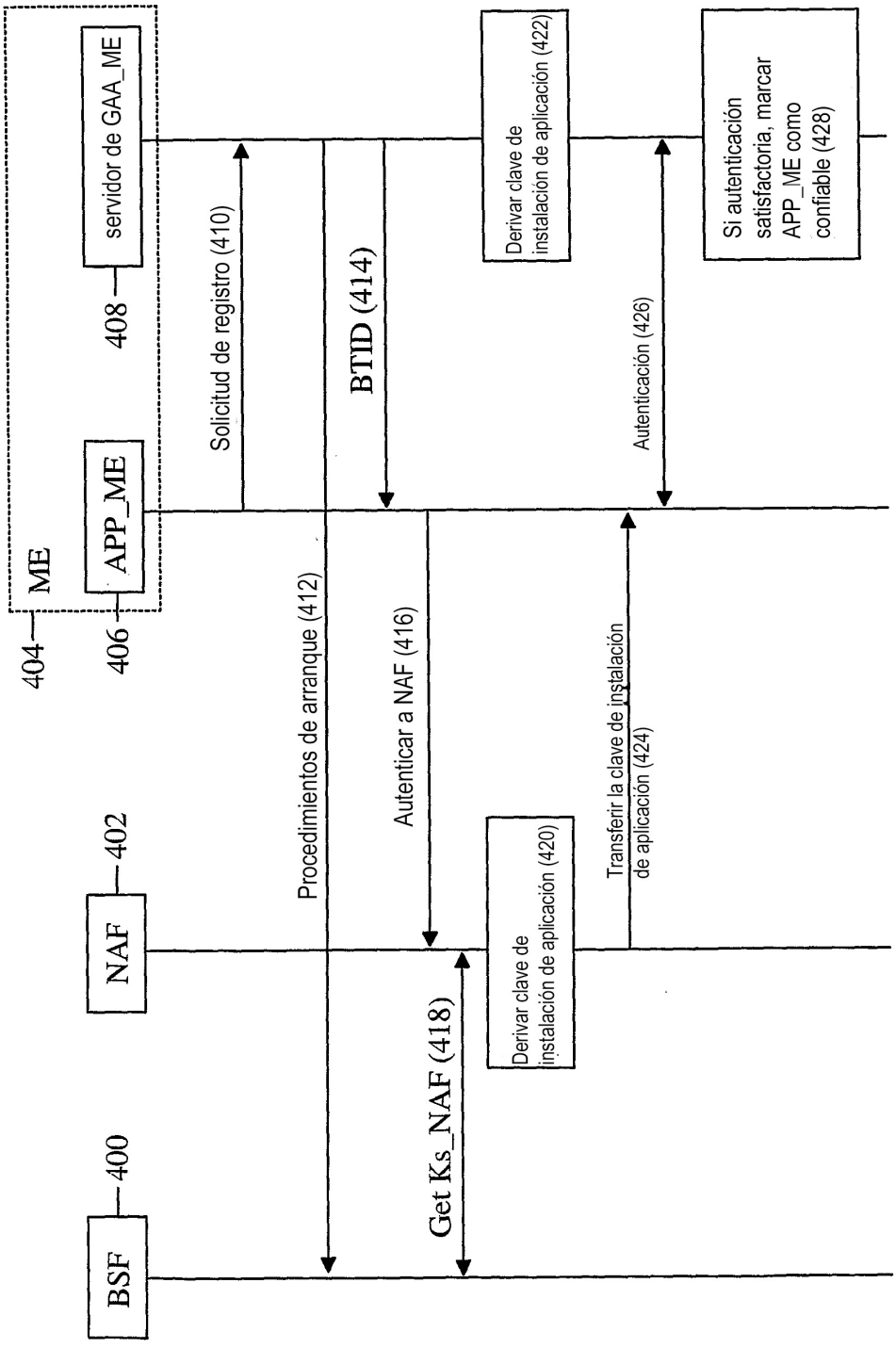
ME
404
APP_ME
406
servidor de GAA_ME
408
NAF
402
BSF
400
Solicitud de registro (410)
Procedimientos de arranque (412)
BTID (414)
Autenticar a NAF (416)
Get Ks_NAF (418)
Derivar clave de instalación de aplicación (420)
Derivar clave de instalación de aplicación (422)
Transferir la clave de instalación de aplicación (424)
Autenticación (426)
Si autenticación satisfactoria, marcar APP_ME como confiable (428)

Fig. 4

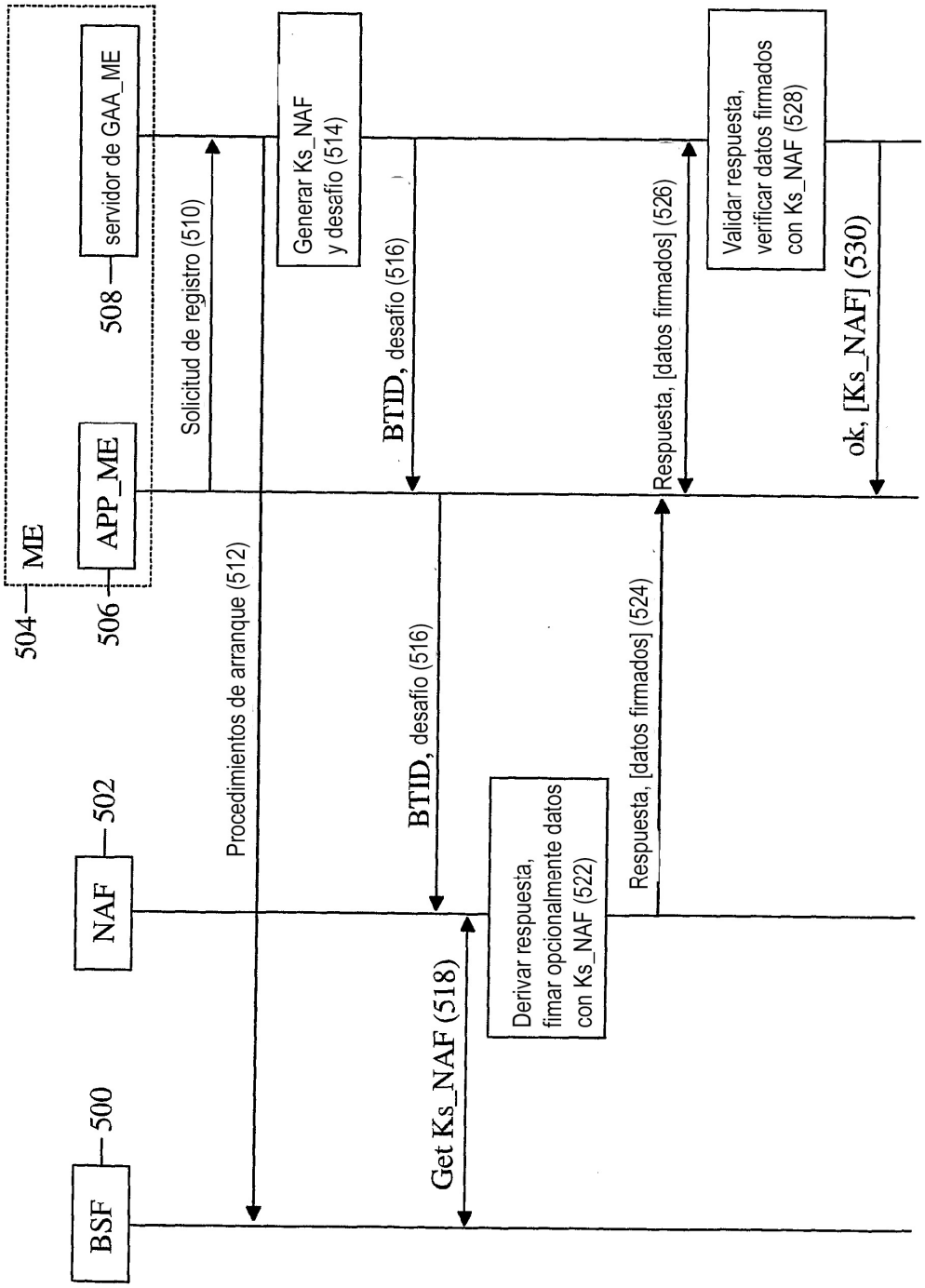
ME
504
APP_ME
506
servidor de GAA_ME
508
BSF
500
NAF
502
Solicitud de registro (510)
Procedimientos de arranque (512)
Generar Ks_NAF y desafío (514)
BTID, desafío (516)
BTID, desafío (516)
Get Ks_NAF (518)
Derivar respuesta, firmar opcionalmente datos con Ks_NAF (522)
Respuesta, [datos firmados] (524)
Respuesta, [datos firmados] (526)
Validar respuesta, verificar datos firmados con Ks_NAF (528)
ok, [Ks_NAF] (530)

Fig. 5