Plataforma de Autenticación basada en Tarjetas ISIM para Redes de Acceso Fijo Residencial

Joaquín López Rizaldos (jolo@tid.es), Francisco Rodríguez García (frg@tid.es), Alejandro Fandiño Orgeira (orgeira@tid.es), Mónica Fernández Pérez (mfp@tid.es), Alejandro García Henderson (alejgm@tid.es)

Telefónica I+D

***Abstract* — Internet access lines have evolved to Ethernet-based networks in last few years. Ethernet access networks are more convenient for new Internet applications, like IPTV services, but current authentication mechanisms are oriented to point to point access networks. Therefore, it's needed to deploy new authentication mechanisms which allow taking advantage of Ethernet features, like multicast transmission. Many solutions have been proposed, most of them based on DHCP Option 82, where the physical access line identifies the user. In this paper is proposed a new authentication scheme where the user identity resides in an ISIM card, in a similar manner as it is done in mobile platforms.**

I. Introducción

En los últimos años las redes de acceso a Internet ATM han comenzado a ser sustituidas por redes basadas en Ethernet [1]. Esta evolución es debida fundamentalmente a dos motivos. En primer lugar, destaca el despliegue masivo de aplicaciones basadas en la transmisión multicast, entre las que destaca principalmente IPTV. Las redes ATM son de naturaleza punto a punto, lo que las hace ineficientes para este tipo de tráfico. A esto hay que añadirle el gran éxito que la tecnología Ethernet ha tenido en redes de área local, lo que la convierte en una tecnología consolidada y asequible.

Este cambio hace necesario diseñar nuevos mecanismos de autenticación para usuarios fijos, ya que hasta ahora se emplea el protocolo PPP, orientado también a conexiones punto a punto, y que a pesar de ser compatible con redes Ethernet (PPPoE), no es eficiente para tráfico multicast. Se han realizado diversas propuestas, la mayor parte de ellas basadas en el protocolo DHCP, añadiendo en el nodo de acceso el identificador de la línea de acceso del usuario en la opción 82 [2].

Aunque a corto plazo es una opción viable, es deseable buscar un mecanismo de autenticación en el que la identidad del usuario no resida en la línea por la que accede, ya que esto tiene varios inconvenientes. Desde el punto de vista del usuario, los servicios están asociados a su línea de acceso, por lo que no puede utilizarlos desde otro acceso, como pudiera ser una segunda residencia. Desde el punto de vista del operador, es necesario provisionar a los usuarios incluso en los equipos de red (DSLAM para ADSL, OLT para FTTx o incluso en el B-RAS), lo que convierte estos procesos en lentos y costosos.

En este artículo se va a presentar una propuesta de autenticación basada en EAP/AKA sobre 802.1X, donde la identidad del usuario reside en una tarjeta ISIM, al igual que sucede en las plataformas de telefonía móvil.

II. Estado Del Arte y Trabajo Relacionado

Existen diversas propuestas que permiten la autenticación de usuarios residenciales mediante mecanismos que desligan la identidad del usuario de la línea física de acceso, permitiendo el nomadismo de los servicios y eliminando la provisión de usuarios necesaria en los equipos de red.

En primer lugar, el protocolo PANA (Protocol for Carrying Authentication for Network Access) [3] propone utilizar el protocolo de transporte de autenticación EAP por encima del nivel IP. De esta forma, el protocolo de autenticación es totalmente independiente de la red de acceso y permite utilizar cualquier algoritmo de autenticación que pueda encapsularse dentro del protocolo EAP. Sin embargo, este mecanismo tiene dos inconvenientes. En primer lugar, es necesario asignar en primer lugar una dirección IP a un usuario que no ha sido previamente autenticado, lo que impide una gestión eficiente de las direcciones IP y aumenta la vulnerabilidad de la plataforma ante ataques, como pueden ser *IP/MAC Spoofing* o *DoS (Denial of Service)*. Además, es necesario que el B-RAS implemente la entidad PAA (PANA Authentication Agent) del protocolo PANA, con lo que sería necesario actualizar los equipos de red.

El protocolo sPANA (Simplified PANA) [4] es una modificación del protocolo PANA que permite que la autenticación del usuario se produzca antes del proceso de asignación de una dirección IP. Esta solución solventa parcialmente los inconvenientes que presenta el protocolo PANA, puesto que sigue necesitando que los equipos de red (B-RAS) implementen la entidad PAA.

Otra solución similar consiste en enviar los mensajes EAP directamente sobre UDP (EAPoUDP) [5], aunque sigue presentando las mismas desventajas detalladas anteriormente.

Por último, existen diversas soluciones como la presentada en [6] que proponen utilizar el protocolo 802.1X para la autenticación del acceso en redes fijas de acceso residencial, de forma similar a como se detalla en este trabajo. Sin embargo, el acceso del usuario a cada servicio debe ser autenticado independientemente y los dispositivos requieren una configuración específica para el acceso a dichos servicios (por ejemplo, encapsulado VLAN y flags de priorización). La propuesta que se detalla en este trabajo da un paso más, presentando un mecanismo de autenticación y de aplicación de políticas de QoS y control de acceso iniciales en las que toda la configuración, tanto de servicios como de políticas, se aplica sobre la red de acceso del usuario, sin requerir ninguna configuración adicional en los dispositivos del usuario. De esta forma el usuario puede acceder a los servicios que tiene contratados desde cualquier dispositivo sin requerir ninguna configuración ad-hoc y sin añadir ninguna complejidad a sus dispositivos o a su red local, siendo también posible el acceso simultáneo a diversos servicios desde un mismo dispositivo. Además, la arquitectura presentada es totalmente compatible con la Release 2 definida por TISPAN y puede ser adoptada fácilmente, ya que no requiere la incorporación de protocolos o mecanismos no soportados por los equipos actuales.

III. Arquitectura NGN Tispan

Para diseñar una nueva plataforma de autenticación para redes fijas es imprescindible tener en cuenta la arquitectura TISPAN, ya que se ha convertido en el estándar de referencia para este tipo de plataformas. La arquitectura completa definida en la Release 2 se define en [7], aunque solo se detallará en este artículo el subsistema NASS [8], encargado de la autenticación de los usuarios:

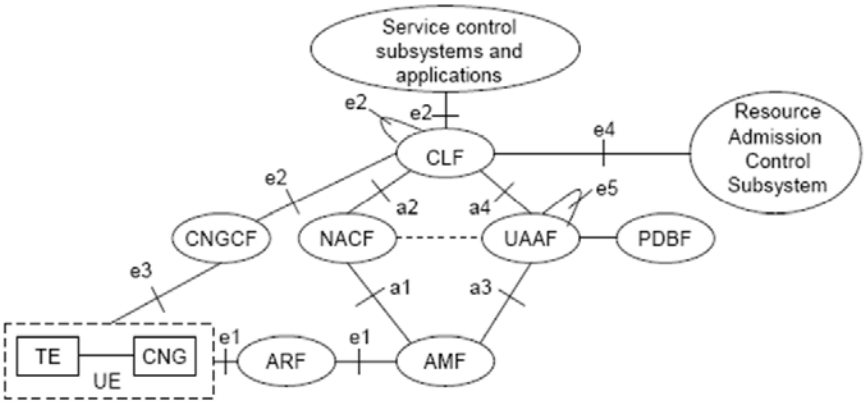

Fig. 1. Arquitectura del subsistema NASS (TISPAN NGN Framework Release 2).

Los elementos que forman el subsistema NASS son los siguientes:

- ARF (*Access Relay Function*): Es implementada en el nodo de acceso (DSLAM/OLT) e inserta información sobre la localización del usuario en las peticiones de autenticación y de asignación de dirección IP enviadas por el usuario.
- AMF (*Access Management Function*): Es el mediador entre el usuario y los servidores de autenticación (*User Access Authorization Function*, UAAF) y de asignación de direcciones IP (*Network Access Configuration Function*, NACF). Su función es recibir las peticiones que provienen del usuario y mapearlas en mensajes que enviará a los servidores correspondientes.
- UAAF: Implementa las funciones AAA (autenticación, autorización y accounting). Para la autenticación y autorización del usuario consulta la identidad y el perfil de red del usuario de la base de datos (*Profile Database Function*, PDBF).
- PDBF: Almacena los datos de autenticación y el perfil de red del usuario, compuesto principalmente de parámetros de QoS (QoS Profile) y políticas de control de acceso (Initial Gate Settings).
- NACF: Su principal función es asignar a los usuarios las direcciones IP, así como otros parámetros de configuración: dirección IP de los servidores de DNS, dirección IP del proxy P-CSCF…
- CLF (*Connectivity Session Location and Repository Function*): Este módulo recoge la información de sesión de los usuarios y permite a las capas de aplicaciones y servicios recibir información de la sesión del usuario en tiempo real (interfaz e2 [9]). También recibe las notificaciones del UAAF y el NACF, y una vez que el usuario es autenticado y recibe los parámetros de configuración necesarios para acceder a la red, solicita la aplicación de las políticas de QoS y control de acceso al RACS (concretamente al elemento A-RACF) a través el interfaz e4 [10].

IV. Propuesta de Autenticación EAP/AKA sobre 802.1X

A continuación se va a presentar una propuesta para la autenticación de usuarios en redes fijas. Se ha tomado la decisión de utilizar dos protocolos durante la fase de autenticación: (1) EAP sobre 802.1X para el transporte de autenticación y (2)

EAP/AKA para la autenticación del usuario. De esta forma el mecanismo de autenticación (AKA) es totalmente transparente para los dispositivos de red, facilitando una posible migración y un futuro despliegue de nuevos mecanismos de autenticación. Una vez autenticado el usuario, la fase de conexión se completará con la asignación de la dirección IP del usuario, para lo que se utilizará DHCP.

Conviene resaltar que aunque para el diseño y la implementación de la solución se ha escogido el protocolo de autenticación AKA, podría ser válido y extensible para cualquier otro algoritmo (por ejemplo SIM o TLS), ya que el transporte de la autenticación (protocolo EAP) es común y por tanto, los algoritmos de autenticación solamente deben ser implementados en el cliente (Home Gateway) y el servidor (Servidor AAA), puesto que son totalmente transparentes para los equipos de red.

La solución propuesta está basada en la arquitectura definida por TISPAN en la Release 2, proponiendo la definición de algunos interfaces que aún no ha sido realizada por TISPAN, como es el caso de los interfaces a1, a3 y a4. Los interfaces a2 [11] y Re [12] tampoco han sido definidos por TISPAN, pero la implementación se basará en los drafts publicados.

A. Arquitectura de la plataforma de autenticación EAP/AKA sobre 802.1X

La arquitectura de autenticación propuesta en este artículo se detalla en la Figura 2, donde se representa superpuesta sobre la arquitectura de TISPAN para mostrar que la plataforma diseñada sigue las recomendaciones publicadas por TISPAN:

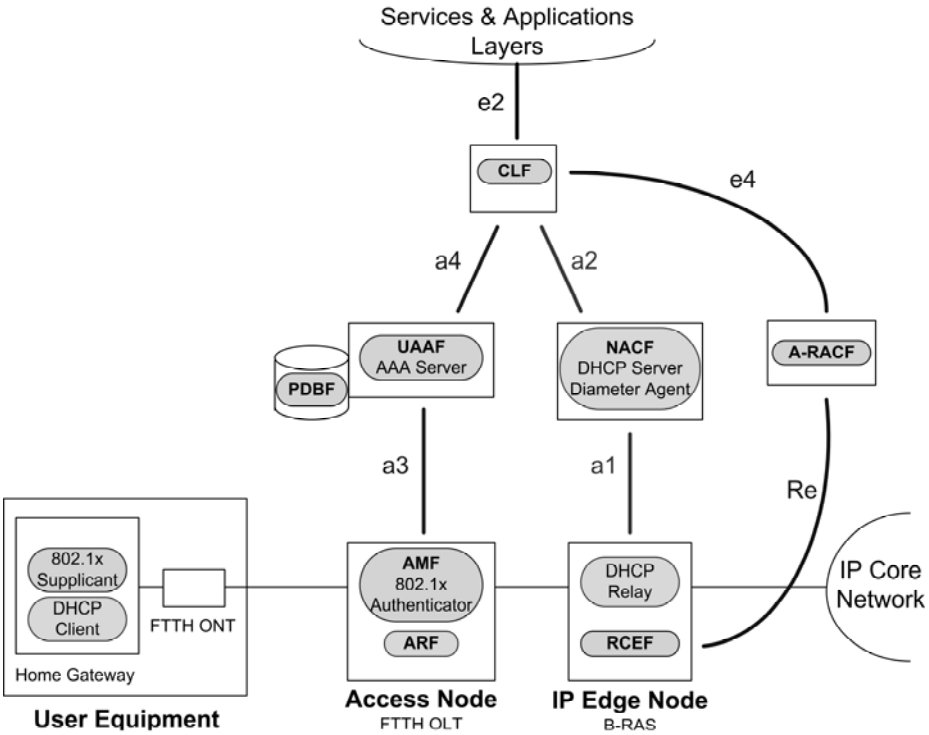

Fig. 2. Propuesta de arquitectura de autenticación basada en EAP/AKA sobre 802.1X.

El Home Gateway del usuario implementará la función de *Supplicant* dentro del protocolo 802.1X, solicitando a la red la autenticación del usuario. También implementará la función de cliente EAP/AKA, aunque esta funcionalidad se ejecutará en la tarjeta ISIM. Por último, actuará como cliente DHCP para una vez que el usuario esté autenticado, obtener una dirección IP que le permita acceder a Internet.

En el nodo de acceso se implementará la función de *Authenticator* de 802.1X (AMF), encargándose de mapear las peticiones EAP del usuario en mensajes RADIUS que enviará al UAAF y viceversa. También se implementará en el nodo de acceso la función ARF, que añadirá en la opción 82 de DHCP el identificador de la línea de acceso, lo cual a su vez permitirá al CLF distinguir las peticiones que pertenecen al mismo usuario, como se describirá posteriormente.

El servidor UAAF se encargará de implementar la autenticación del usuario (EAP/AKA), obteniendo los datos del usuario de la base de datos (PDBF). Ambos notificarán al CLF cuando los procesos de autenticación y asignación de dirección IP hayan concluido satisfactoriamente. El CLF será capaz de discernir cuándo las peticiones pertenecen al mismo usuario, y en tal caso solicitará al A-RACF que aplique las políticas de QoS y control de acceso del perfil del usuario, lo que finalmente se efectuará en el B-RAS (módulo RCEF). Además, el CLF permitirá, a las capas de aplicación y de servicios, recuperar los datos de las sesiones de usuario en tiempo real, a través del interfaz e2.

B. Flujo de autenticación inicial y asignación de dirección IP

A pesar de que han sido implementados los mecanismos correspondientes a una sesión de usuario completa (autenticación, re-autenticación y terminación de sesión) en este artículo sólo se va a detallar el proceso de autenticación inicial debido a la limitación de espacio.

El proceso de autenticación está dividido en tres fases: en primer lugar, se ejecuta el algoritmo EAP/AKA para permitir el acceso del usuario a la red, a continuación se ejecuta el procedimiento de asignación de dirección IP basado en DHCP, y por último el CLF se encargará de solicitar la aplicación de las políticas de QoS y control de acceso al RACS.

En la Figura 3 se detalla el proceso de autenticación EAP/AKA sobre 802.1X:

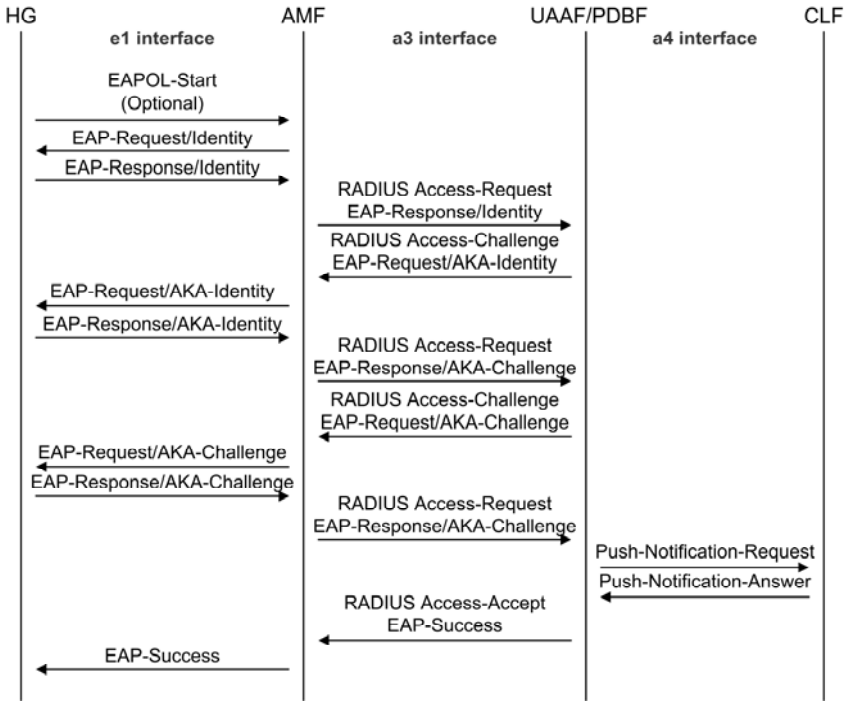

Fig. 3. Flujo de autenticación basado en EAP/AKA sobre 802.1X.

En primer lugar, el protocolo 802.1X [13] filtra en el nodo de acceso todo el tráfico proveniente de un usuario no autenticado y le solicita que lance el proceso de autenticación (*EAP-Request/Identity*). A continuación el usuario lanza un mensaje con su identidad (*EAP-Response/Identity*), que el nodo de acceso mapea a un mensaje RADIUS y envía la petición al servidor AAA (UAAF). El servidor UAAF seleccionará entonces el mecanismo de autenticación que desea ejecutar, y de esta forma comienza el proceso de autenticación EAP/AKA [14], [15]. El UAAF obtiene los datos del usuario (mecanismo de autenticación, claves privadas, etc) del PDBF.

Una vez que finaliza el proceso de autenticación, el servidor UAAF notificará al CLF que el usuario ha sido correctamente autenticado, y le enviará el perfil de acceso del usuario (QoS Profile y Initial Gate Settings). Cuando el nodo de acceso (AMF) recibe la notificación de que el usuario ha sido autenticado correctamente (*EAP-Success*), eliminará los filtros que filtraban el tráfico del usuario.

En la siguiente fase, el cliente DHCP solicita una dirección IP que le permita el acceso a Internet (Figura 4). El servidor NACF se encargará de asignar las direcciones IP a los clientes, y una vez que haya asignado la dirección IP del usuario, lo notificará al CLF.

El CLF recibirá las notificaciones del UAAF y del NACF, con lo que una vez que el usuario se haya autenticado y haya recibido la dirección IP, solicitará al A-RACF que aplique las políticas de acceso correspondientes del usuario a través del interfaz e2, tal y como se detalla en [10]. El A-RACF se encargará de solicitar al módulo RCEF (B-RAS) la aplicación de estas políticas a través del interfaz Re [12].

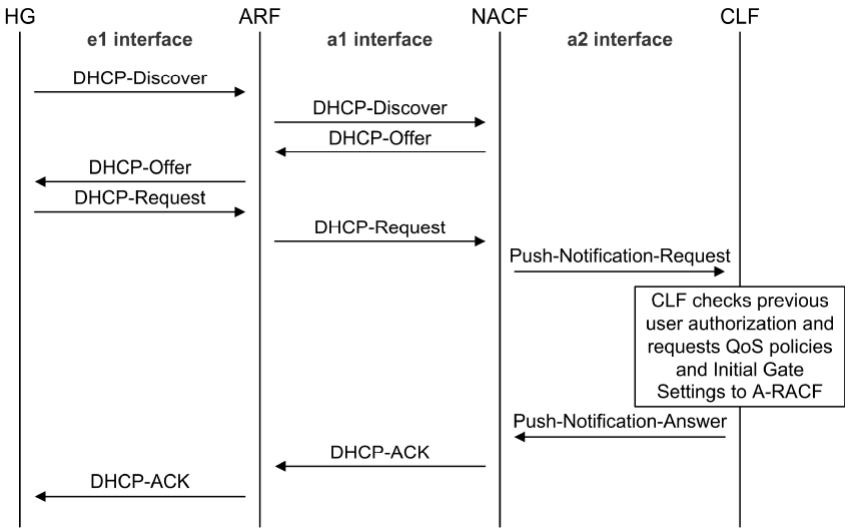

Fig. 4. Flujo de asignación de dirección IP basado en el protocolo DHCP.

El CLF deberá discernir si las notificaciones que recibe del UAAF y del NACF pertenecen al mismo usuario. Para ello, el ARF deberá insertar en las peticiones de autenticación (RADIUS) y de asignación de dirección IP (DHCP) un identificador único por usuario, que posteriormente progresará al CLF. En la implementación se ha seleccionado el puerto lógico por el que accede el usuario, que es mapeado al atributo RADIUS NAS-Port y a la opción 82 del protocolo DHCP. Es importante resaltar que este atributo solamente es utilizado en el CLF para correlar las peticiones que pertenecen a un mismo usuario, pero es totalmente transparente para la operadora, y por tanto, no debe ser provisionado en los sistemas de red o de identificación y autenticación de usuarios.

V. Conclusión

Este artículo resume algunos de los aspectos más relevantes de diseño e implementación de una plataforma de autenticación basada en EAP/AKA sobre 802.1X. El desarrollo ha sido validado en una red de acceso GPON FTTH 7342 ISAM de Alcatel, utilizando como B-RAS el agregador ERX-710 de Juniper.

En el mecanismo de autenticación desarrollado en este trabajo, la identidad del usuario queda ligada a una tarjeta ISIM, en lugar de la línea física de acceso, tal y como se hace hasta ahora. Esto simplifica, desde el punto de vista del operador, la provisión de usuarios. Desde el punto de vista del usuario, permite un mayor grado de flexibilidad en los servicios, añadiendo ubicuidad. Por ejemplo, el usuario podría utilizar su servicio de acceso a Internet o disfrutar de los contenidos comprados en una plataforma IPTV desde cualquier otra ubicación, como puede ser una segunda residencia.

También se ofrece un mecanismo de autenticación mucho más seguro que el empleado actualmente, muy similar al empleado en las plataformas móviles. Esta solución podría ser un primer paso en la convergencia fijo-movil, ya que permitirá a ambos tipos de redes compartir los sistemas de autenticación.

Por último, la solución propuesta es totalmente compatible con la arquitectura presentada en la Release 2 de TISPAN, asegurando la interoperabilidad y la compatibilidad. También se garantiza una migración sencilla desde las redes de acceso actuales, ya que el mecanismo 802.1X ya está implementado en la mayor parte de los nodos de acceso que las operadoras tienen desplegados, y el mecanismo de autenticación EAP/AKA es completamente transparente para los dispositivos de red, siendo únicamente necesaria su implementación en el servidor AAA y en el Home Gateway del cliente.

Referencias

[1] DSL Forum TR-101, *Migration to Ethernet-Based DSL Aggregation*, Abril 2006.

[2] Internet Draft, *Authentication Extensions for the Dynamic Host Configuration Protocol (draft-pruss-dhcp-auth-dsl-02)*, November 2007.

[3] RFC 5191, *Protocol for Carrying Authentication for Network Access (PANA)*, Mayo 2008.

[4] Internet Draft, *Simplified Protocol for Carrying Authentication for Network Access (sPANA) (draft-xia-pana-simplified-00.txt)*, Febrero 2008.

[5] Internet Draft, *EAP over UDP (EAPoUDP) (draft-engelstad-pana-eap-over-udp-00.txt)*, Febrero 2002.

[6] Jon Matias, Eduardo Jacob, Mariví Higuero, Purificación Saiz, Jorge Martínez de Salinas; "*Una propuesta basada en IEEE 802.1X para la autenticación y configuración de equipos finales en redes NGN*"; Telecom I+D 2007, Octubre 2007.

[7] ETSI ES 282 001 V1.1.1, *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 2.*

[8] ETSI ES 282 004 V1.1.1, *Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Subsystem (NASS).*
[9] ETSI ES 283 035 V2.5.0, *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol.*
[10] Draft ETSI ES 283 034 V1.5.0, *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol.*
[11] Draft ETSI TS 183 059-1 V0.5.1, *Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN) Network Attachment Subsystem a2 interface based on the DIAMETER protocol.*
[12] Draft ETSI TS 183 060 V0.4.0, *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Subsystem (RACS); Re interface based on the DIAMETER protocol.*
[13] *IEEE Standard for Local and metropolitan area networks, Port-based Network Access Control, IEEE Standard 802.1X*, Diciembre 2004.
[14] RFC 3748, *Extensible Authentication Protocol (EAP)*, Junio 2004.
[15] RFC 4187, *Extensible Authentication Protocol for 3rd Generation Authentication and Key Agreement, Internet Society*, Enero 2006.