

En este artículo se describe por una parte la estructura y componentes principales de UMTS: dominios y puntos de referencia. Se identifica la arquitectura de seguridad de la Tercera Generación en Móviles 3G/UMTS, mostrando las capas y relaciones entre entidades; también se ubica la funcionalidad de PKIs/TTPs a la hora de poder aplicar criptografía de clave pública en un entorno UMTS. Asimismo, se aborda UMTS desde la perspectiva de la seguridad. UMTS puede ofrecer servicios multimedia, permite navegar por Internet y posibilita trabajar con redes inalámbricas, alámbricas, terrenas y vía satélite. UMTS definido por el ETSI (*European Telecommunications Standards Institute*) fue seleccionado por la ITU (*International Telecommunication Union*) como sistema del estándar IMT2000 (*International Mobile Telecommunications 2000*) para la definición de los sistemas móviles de la tercera generación.

Análisis en torno a la arquitectura global de seguridad en UMTS

UMTS está suscitando grandes expectativas entre los operadores de redes móviles, nuevos proveedores de servicios y de contenidos, y algunos usuarios conscientes del gran impacto que pueden ocasionar los avances tecnológicos de la 3G de móviles en sus negocios e intereses. En un escenario donde muchos operadores están apostando por redes IP para su red fija, el tener la posibilidad de disponer de una red móvil también basada en IP, nos puede aproximar hacia la tan deseada convergencia de redes fijas y móviles que podrán compartir muchos de los recursos de la red.

En un futuro próximo los operadores podrán ofrecer servicios Internet con acceso optimizado entre UMTS y redes IP externas. El amplio abanico de posibles nuevos servicios móviles multimedia personalizados y la alta calidad que UMTS podrá ofrecer, está originando un crecimiento de expectativas en este nuevo enfoque de comunicaciones celulares, pero no se debe olvidar el Factor Seguridad que tiene que presidir esta evolución y migración de GSM (2G) a través de GPRS (2,5G) al UMTS (3G). En este sentido la figura 1 especifica un esquema que muestra la arquitectura de seguridad de UMTS como guía para el desarrollo de políticas de seguridad modernas, estructuradas, acordes con las necesidades cambiantes de los consumidores, comerciantes, operadores, proveedores de servicio y demás agentes implicados con las telecomunicaciones.

ESTRUCTURA DE UMTS: DOMINIOS Y PUNTOS DE REFERENCIA

La arquitectura general de UMTS se puede definir utilizando un modelo de dominios, capas y puntos de referencia. Un dominio es una agrupación de nodos físicos. Los puntos de referencia se definen entre pares de dominios. Los interfaces en estas fronteras deberían estandarizarse para posibilitar un interfuncionamiento entre equipos de diferentes fabricantes. Por último, una capa o nivel es la agrupación de protocolos relacionados con un aspecto de los servicios y lo proporciona normalmente alguna funcionalidad de uno o varios dominios.

La arquitectura UMTS –véase la figura 2– se puede dividir en dos dominios: UE (User Equipment) y IE (Infrastructure Equipment). Esta primera subdivisión establece la diferencia entre UE que normalmente está dentro de las premisas de los usuarios finales y el IE que opera para beneficio de un colectivo de usuarios. En una implementación que ofrece movilidad, la frontera entre los dos dominios es el lugar principal donde dicha movilidad se ofrece a los usuarios. UE es el

equipo utilizado por el usuario para acceder a los servicios UMTS. Este dominio engloba una gran variedad de tipos de equipos (móviles, fijos, etc.) con diferentes niveles de funcionalidad y puede ser compatible con uno o

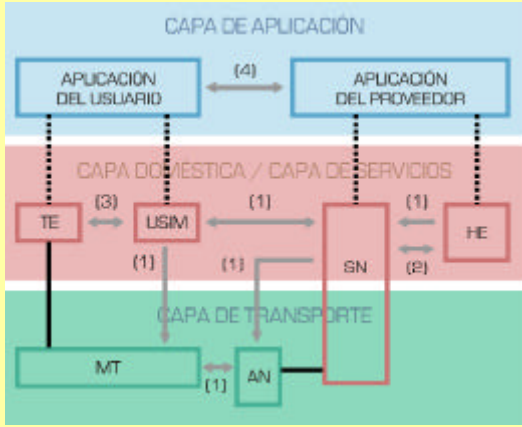


Fig. 1.- Diagrama General de Bloques de la Arquitectura de Seguridad de 3G/UMTS.

más interfaces de acceso existentes, por ejemplo, UE con modo dual UMTS-GSM.

El UE incluye el ME (Mobile Equipment) y uno o más USIMs (User Services Identity Modules); el dominio UE se subdivide en dominio ME y dominio USIM. El punto de referencia entre el ME y el USIM se denomina «Cu». El dominio USIM contiene la funcionalidad utilizada para acceder a los servicios UMTS de una cierta red doméstica HN. El USIM es una aplicación que puede residir en una tarjeta inteligente removible que puede contener otras aplicaciones. También puede no ser removible y estar integrada en el equipo móvil. El USIM contiene datos y procedimientos que le identifican de forma segura y sin ambigüedad y están normalmente incluidos en una tarjeta inteligente. El ME realiza la funcionalidad de transmisión de radio en el lado del usuario y contiene aplicaciones extremo a extremo.

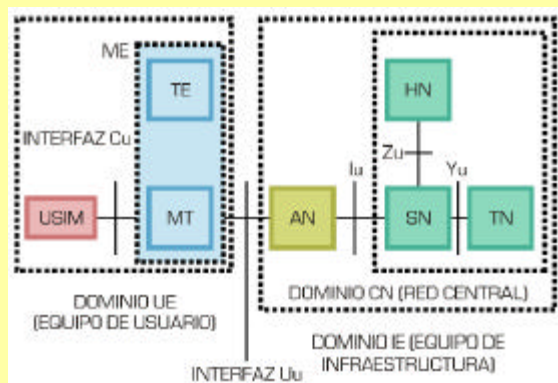
Por su parte, el dominio ME se subdivide en dos sub-dominios: i) TE (Terminal Equipment), que contiene la funcionalidad relativa a las aplicaciones extremo a extremo (por ejemplo, micrófono, altavoz, pantalla de un laptop-computer) y ii) MT (Mobile Termination), que contiene la funcionalidad relativa a la transmisión de radio. El punto de referencia «Uu» entre UE y IE se realiza por un interfaz de acceso concreto.

UMTS puede proporcionar más de un interfaz de acceso, sin embargo, sólo un interfaz terrestre de radio se desarrolla, el denominado UTRA (UMTS Terrestrial Radio Access). Otros interfaces de acceso podrán ser estandarizados, por ejemplo para proporcionar acceso vía satélite o a través de red fija. El dominio IE consta de nodos físicos que realizan las diversas funciones requeridas para terminar el interfaz de radio y soportar los servicios de telecomunicaciones que precisan los usuarios. El dominio IE es un recurso compartido que proporciona servicios a todos los usuarios finales autorizados dentro de su área de cobertura. El dominio IE se subdivide a su vez en el dominio AN (Access Network), que se caracteriza por estar en contacto directo con el UE y el dominio CN (Core Network). Esta subdivisión ayuda a desacoplar la funcionalidad relativa al acceso de la funcionalidad relacionada con cuestiones que no son de acceso y se encuentra en sintonía con el principio modular adoptado por la UMTS que especifica qué partes de la red deberían permitirse desarrollarse de forma independiente. El dominio AN comprende las funciones específicas para la técnica de acceso, mientras las funciones del dominio CN se pueden utilizar con flujos de información que utilizan cualquier técnica de acceso. Esta división permite diferentes enfoques para la red CN, cada enfoque especifica distintos tipos de CNs conectables al dominio AN, así como diferentes técnicas de acceso, cada tipo de AN conectable al

dominio CN. Otro argumento para dicha división total física es el funcionamiento potencial independiente de ANs y CNs.

El punto de referencia entre AN y CN se denomina «Iu». El dominio AN (Access Network) consta de los nodos físicos que gestionan los recursos de las ANs y proporciona al usuario un mecanismo para acceder al dominio CN. Una red AN puede proporcionar movilidad, por ejemplo como UTRAN. Otros ejemplos de AN son las redes de líneas fijas y las redes vía satélite. El dominio CN consta de los nodos físicos que proporcionan soporte para las características de red y los servicios de telecomunicaciones. El soporte proporcionado incluye funcionalidad de gestión de información de localización de usuarios, control de las características y servicios de red, los mecanismos de transferencia (conmutación y transmisión) para señalización y para información generada por el usuario. El dominio CN se subdivide en el dominio SN (Serving Network), el dominio HN (Home Network) y el dominio TN (Transit Network). El punto de referencia entre SN y la HN se denomina «Zu». El punto de referencia entre SN y la TN se denomina «Yu».

SN, TN y HN se interpretan como los «roles» (funciones) que pueden desempeñar ciertas redes en relación a una cierta llamada. Las redes pueden tener la capacidad de desempeñar más de un «rol» y para una única llamada no son necesariamente diferentes. El dominio SN (Serving Network) es la parte del dominio CN al que esta conectada la AN que proporciona el acceso de usuario. Representa las funciones de CN que son locales al punto de acceso del usuario y por tanto su localización cambia cuando el usuario se mueve. La red SN es la responsable de encaminar llamadas y transportar la información/datos del usuario desde la fuente al destino. Tiene la capacidad de interactuar con la HN para atender los servicios/datos específicos del usuario y con la red TN para propósitos de servicios/datos específicos que no son de usuario. El dominio HN (Home Network) representa las funciones de la red CN que son guiadas a una localización permanente sin tener en cuenta la localización del punto de acceso del usuario. El USIM esta relacionado por la suscripción con la red HN. La red HN contiene al menos datos específicos de usuario de forma permanente y es responsable de la gestión de la información de suscripción. También puede gestionar servicios específicos de HN, potencialmente no ofrecidos por el dominio SN. El dominio TN (Transit Network) es la parte del dominio CN localizado en el camino de comunicación entre la red SN (HN) y la parte remota. Si para una llamada dada la parte remota está localizada dentro de la misma red como el UE originador, entonces no se activa ninguna instancia particular del dominio TN.



PUNTOS DE REFERENCIA/INTERFACES:

Cu : USIM (User Services Identity Module) - ME (Mobile Equipment)

Uu : UE (User Equipment) - IE (Infrastructure Equipment)

Iu : AN (Access Network) - SN (Serving Network)

Yu : SN - TN (Transit Network)

Zu : SN - HN (Home Network)

DOMINIOS:

ME = TE (Terminal Equipment Domain) + MT (Mobile Termination Domain)

UE = ME + USIMs

IE = AN + CN (Core Network)

CN = HN + SN + TN

ARQUITECTURA UMTS = UE + IE

Fig. 2.- Esquema de dominios y puntos de referencia de la arquitectura UMTS.

El dominio SN (Serving Network) es la parte del dominio CN al que esta conectada la AN que proporciona el acceso de usuario. Representa las funciones de CN que son locales al punto de acceso del usuario y por tanto su localización cambia cuando el usuario se mueve. La red SN es la responsable de encaminar llamadas y transportar la información/datos del usuario desde la fuente al destino. Tiene la capacidad de interactuar con la HN para atender los servicios/datos específicos del usuario y con la red TN para propósitos de servicios/datos específicos que no son de usuario. El dominio HN (Home Network) representa las funciones de la red CN que son guiadas a una localización permanente sin tener en cuenta la localización del punto de acceso del usuario. El USIM esta relacionado por la suscripción con la red HN. La red HN contiene al menos datos específicos de usuario de forma permanente y es responsable de la gestión de la información de suscripción. También puede gestionar servicios específicos de HN, potencialmente no ofrecidos por el dominio SN. El dominio TN (Transit Network) es la parte del dominio CN localizado en el camino de comunicación entre la red SN (HN) y la parte remota. Si para una llamada dada la parte remota está localizada dentro de la misma red como el UE originador, entonces no se activa ninguna instancia particular del dominio TN.

IDENTIFICACIÓN DE CLASES DE CARACTERÍSTICAS DE SEGURIDAD EN LA ARQUITECTURA DE SEGURIDAD 3G

La arquitectura de seguridad 3G/UMTS define las clases de características de seguridad siguientes de las cuales las cuatro primeras se especifican numéricamente en la figura 1 :

1) Seguridad de acceso a la red . Es el conjunto de características de seguridad que proporciona a los usuarios acceso seguro a los servicios 3G y en particular protege contra ataques al enlace de acceso vía radio.

2) Seguridad del dominio de red . Es el conjunto de características de seguridad que permite a los nodos del dominio del proveedor intercambiar de forma segura datos de señalización y protege contra ataques en la red fija de naturaleza alámbrica.

3) Seguridad del dominio de usuario . Es el conjunto de características de seguridad que hacen seguro el acceso a la estación móvil (teléfono móvil 3G, PDA (Personal Digital Assistant), HPC (Handheld PC), Palmtop Computer, Laptop Computer, M-Notebook, etc.; Los tipos de estación móvil o MS se pueden clasificar atendiendo a sus capacidades de servicio más que a sus características físicas en: MS sólo para voz, MS para datos de banda estrecha, MS para datos de banda ancha, MS para voz y datos multimedia, etc.).

4) Seguridad del dominio de aplicación . Es el conjunto de características de seguridad que permiten a las aplicaciones del dominio de usuario y del dominio del proveedor intercambiar mensajes de forma segura.

5) Visibilidad y configurabilidad de la seguridad . Es el conjunto de características que permiten al usuario informarle de si las características de seguridad se encuentran operativas o no y si el uso y provisión de los servicios depende de la característica de seguridad.

En la figura 1 se muestran, por una parte, las entidades y enlaces implicados en los grupos de características de seguridad indicados anteriormente, y, por otra parte, las tres capas principales de la arquitectura de seguridad UMTS:

1. Capa de transporte, es la capa inferior y contiene MT (Mobile Termination), AN (Access Network) y SN (Serving Network).

2. Capa domestica/Capa de servicios es la intermedia y contiene TE (Terminal Equipment), USIM (User Services Identity Module), SN (Serving Network) y HE (Home Environment).

3. Capa de aplicación es la superior y contiene las aplicaciones del usuario y las aplicaciones del proveedor.

SEGURIDAD DE ACCESO A LA RED

Esta clase de características de seguridad se compone de las siguientes características:

1) Confidencialidad de la identidad del usuario . Para llevar a cabo la confidencialidad de la identidad de usuario, el mecanismo de GSM (telefonía 2G) utiliza identidades temporales acordadas entre la red SN y el usuario/abonado mantenido. Sin embargo, el mecanismo de GSM permite a la SN pedir que el usuario envíe su identidad de usuario en texto sin cifrar a través del enlace de acceso vía radio. El hecho de que este procedimiento no puede eliminarse posibilita a un atacante activo utilizar un capturador de identidad que revela la identidad del usuario. Un entorno doméstico HE UMTS tiene la opción de proteger a sus usuarios contra dicho

ataque implementando un mecanismo para mejorar la confidencialidad de la identidad de usuario (denominado EUIC, Enhanced User Identity Confidentiality), colocado entre las USIM del usuario y una entidad de red HE denominada UIC (User Identification Centre). Para realizar esto, la SN soportará un mecanismo de transporte para mejorar la confidencialidad de la identidad del usuario. La implementación del mecanismo para la EUIC entre el USIM y el UIC es opcional y el propio mecanismo puede ser de propiedad del HE.

2) Autenticación de entidad (enlace de acceso). La autenticación de entidad para el usuario y red se realiza a través del mecanismo de autenticación UMTS y del mecanismo de acuerdo/gestión de clave (AKA). Las partes que se autentican son el USIM expedido por el HE y el AuC (Authentication Centre) del dominio HE. Además de las características de seguridad proporcionadas por el mecanismo GSM, el mecanismo AKA de UMTS asegura que el usuario sólo acepte datos de autenticación «frescos» (desafío aleatorio y las claves derivadas). Así mismo, el mecanismo genera una clave de cifrado para confidencialidad de datos y una clave de integridad para implantar la integridad de los datos transmitidos a través del enlace de acceso aéreo. El mecanismo usa números de secuencia y contadores ubicados en el AuC y el USIM asegura lo «fresco» (actual/vigente/no repetido) de los datos de autenticación. De acuerdo al estándar ISO/IEC 9798-4, el mecanismo proporciona «autenticación mutua» entre el usuario y la red.

3) Confidencialidad de los datos (enlace de acceso). Al igual que en GSM, en UMTS la confidencialidad de los datos se aplicará a los datos de usuario y a los datos de señalización transmitidos a través del enlace de acceso por radio. Para realizar eso, se implementará un cifrador de flujo en cada extremo del enlace de acceso. Comparado con GSM, el cifrado UMTS terminará en la red y se aplicará a un nivel superior. La longitud de clave de UMTS es mayor que la de GSM33.20.

4) Integridad de datos (enlace de acceso). La primera característica nueva de seguridad de acceso de red en UMTS es la integridad de los datos que se aplicará a los mensajes de señalización seleccionados transmitidos a través del enlace de radio. Para proporcionar esto se implementará una función de autenticación de mensajes en cada extremo del enlace de acceso. Esta característica protege contra el «hijacking» («secuestro») de servicios para autenticar al usuario y red durante y antes de la provisión del servicio y para permitir que ambas partes establezcan de forma segura conexiones sin ejecutar un protocolo AKA (Authentication and Key Agreement).

5) Identificación del equipo de usuario . GSM implementa un mecanismo para la identificación del equipo de usuario pero dicho mecanismo no es seguro. Para disuadir de posibles robos, una característica de personalización entre el USIM y el UE puede proporcionar un mecanismo alternativo, sin implicar las entidades de red. Otra alternativa es ubicar esta característica de seguridad debajo del nivel de aplicación.

6) Cifrado de red . La segunda característica nueva de acceso a red de UMTS/3G es el cifrado de red. Es una extensión de esta característica de seguridad que proporciona un modo protegido de transmisión a los canales de tráfico de usuario a través de toda la red. De este modo proporciona a los usuarios garantía de que sus datos de usuario se encuentren protegidos contra escuchas clandestinas en todos los enlaces de la red, es decir no sólo

en los enlaces de radio particularmente vulnerables de la red de acceso, sino también en los enlaces fijos dentro de la red troncal central. Esta característica se incluye en la categoría de características de seguridad del nivel de aplicación. Sin embargo el mecanismo reutiliza el cifrado para la seguridad de acceso a la red y debería considerarse una característica de seguridad de acceso a red, aunque su objetivo con respecto a la confidencialidad de los datos (enlace de acceso) sea primariamente proteger los datos de usuario cuando se transmiten a través de las conexiones de la red central.

SEGURIDAD DEL DOMINIO DEL PROVEEDOR

Esta clase de características de seguridad contiene las que proporciona a los operadores de red SN y entornos domésticos HE con la capacidad de comunicaciones seguras a través de los enlaces de la red central y monitorizar la utilización de su sistema y detectar y contrarrestar comportamientos fraudulentos. Esta clase abarca:

- 1) Autenticación de entidad (entre las entidades de red central)
- 2) Negociación de claves (entre las entidades de la red central).
- 3) Distribución de claves (entre las entidades de la red central).
- 4) Confidencialidad de datos (de señalización sobre los enlaces de la red central).
- 5) Integridad de datos (de señalización sobre los enlaces de la red central).
- 6) Detección de fraudes. Esta característica recoge información de posibles fraudes para permitir a los operadores detectar y combatir posibles comportamientos fraudulentos.

Las cinco primeras características de seguridad permiten a los nodos del dominio del proveedor autenticar de forma segura y negociar las claves de sesión y a continuación intercambiar de forma segura datos de señalización. Para proporcionar esto, se ha definido un mecanismo que puede utilizarse para hacer seguros los mensajes MAP (Mobile Application Part) de la red de señalización SS7. Estos mecanismos de seguridad proporcionan una característica de seguridad esencial que se requiere antes de que los proveedores UMTS puedan migrar de forma segura de enlaces de señalización dedicados a compartidos, por ejemplo sobre Internet.

SEGURIDAD DEL DOMINIO DE USUARIO

Esta clase contiene aquellas características de seguridad que controlan el acceso al USIM o al terminal y que se encuentran completamente implementadas en el dominio de usuario (UE+USIM):

- 1) Autenticación usuario-USIM . Restringe el acceso al USIM a un usuario autorizado o a un conjunto de usuarios autorizados. Para realizar esto, los usuarios y el USIM deben compartir un secreto (p.e., un PIN o incluso información biométrica: reconocimiento del patrón de voz, reconocimiento del iris, retina, huellas dactilares, distribución de los poros de la piel, geometría de la mano, patrón de colocación de venas de la mano/muñeca, caracterización grafológica de la firma manuscrita, composición química del olor corporal, características de la cara y emisión térmica, composición genética basada en RNA/DNA, etc.) que se almacena de forma segura en el USIM.

- 2) Autenticación USIM-UE . Restringe el acceso al UE a un USIM particular o a un conjunto de USIMs. En este caso el USIM y el UE deben compartir un secreto que se almacena de forma segura en el USIM y en el UE.

SEGURIDAD DEL NIVEL DE APLICACIÓN

Esta clase de características de seguridad proporciona interfaces y subniveles de seguridad que permiten a las aplicaciones establecer comunicaciones de forma segura a través de enlaces vía radio y alámbricos; así, por ejemplo proporciona seguridad de aplicaciones seguras entre las aplicaciones en el dominio del usuario y en el dominio del proveedor. El toolkit de aplicación SIM es un interfaz estandarizado que soporta varios servicios de seguridad (p.e., autenticación de entidad, autenticación de mensajes, detección de repeticiones, garantía de integridad de secuencia, confidencialidad y prueba de recepción).

VISIBILIDAD Y CONFIGURABILIDAD

Aunque en general las características de seguridad deberían ser transparentes al usuario, para ciertos eventos y de acuerdo a los deseos del usuario debería proporcionarse una visibilidad mayor del usuario de la operación de las características de seguridad. Esto puede incluir:

1. Una indicación del cifrado de la red de acceso.
2. Una indicación del cifrado de toda la red.
3. Una indicación del nivel de seguridad 2G/3G, por ejemplo, cuando el usuario pasa de 3G a 2G. Por su parte, la configurabilidad es la propiedad de que el usuario y el HE del usuario puedan configurar si el uso o la provisión de un servicio debería depender de si una característica de seguridad está operativa. Esto puede incluir:
 - Habilitar/inhabilitar la autenticación usuario/USIM para ciertos servicios.
 - Aceptar/rechazar llamadas no cifradas entrantes.
 - Establecer o no llamadas no cifradas.
 - Aceptar/rechazar el uso de ciertos algoritmos de cifrado. Actualmente sólo la indicación de cifrado es la única característica de seguridad definida. Frecuentemente las características de seguridad se implementan en una única entidad de red o proporcionan condiciones frontera pequeñas en las características y mecanismos de seguridad existentes y pueden incluirse en la descripción de ellas.

CATEGORÍAS DE SERVICIOS DE SEGURIDAD UMTS QUE UTILIZAN PKI

UMTS precisa de PKI para poder gestionar claves y certificados. Tres son las categorías de características de seguridad que puede proporcionar la arquitectura de seguridad UMTS:

- 1) Seguridad del acceso a red . Esta categoría engloba todas las características de seguridad proporcionadas para proteger el acceso básico a los servicios portadores de telecomunicaciones en UMTS. Las características de seguridad son: autenticación mutua, establecimiento de la clave de sesión para la protección del canal de tráfico subsiguiente, y la protección de la confidencialidad de la identidad y localización.

2) Seguridad extremo a extremo entre usuarios y VASPs (Value Added Service Providers). Esta categoría recoge todas de las características de seguridad proporcionadas para proteger las comunicaciones extremo a extremo sobre los servicios portadores UMTS subyacentes entre un usuario y un VASP. Normalmente estas características de seguridad deberían ser proporcionadas como una parte integral del servicio de valor añadido.

3) Seguridad extremo a extremo entre usuarios . Esta categoría integra todas las características de seguridad proporcionadas para proteger las comunicaciones extremo a extremo bajo los servicios portadores UMTS subyacentes entre usuarios. Normalmente estas características de seguridad deberían ser proporcionadas como una parte integral del servicio de usuario final.

SEGURIDAD DE RED: ROLES Y SU INTERRELACIÓN

La aplicación de la criptografía de clave pública para proporcionar seguridad en el acceso a red permite identificar tres «roles»:

1. Usuarios . Es el «rol» o entidad que está autorizada para utilizar los servicios UMTS debido a la existencia de una asociación con un HE. En UMTS un usuario se identifica y autentica usando un USIM.

2. HE (Home Environment). Es el «rol» que tiene responsabilidad global de proporcionar un servicio a los usuarios con el que tiene una asociación. Esto incluye la provisión, asignación y gestión de cuentas de usuario y los mecanismos necesarios para facturar a los usuarios por sus cargos y para pagar a las redes SNs por los cargos de los usuarios. También incluye la negociación con las redes de las capacidades necesarias para proporcionar servicios UMTS a sus usuarios, incluyendo acuerdos «fuera de línea» que permiten la provisión de servicios y la interacción «en línea» para asegurar que los usuarios se encuentren adecuadamente identificados, localizados, autenticados y autorizados a la hora de utilizar los servicios portadores antes de que dichos servicios se les proporcionen.

3. SN (Serving Network). Es el «rol» que proporciona recursos de radio, gestión de la movilidad y capacidades fijas para conmutar, encaminar y manipular los servicios ofrecidos a los usuarios. Las capacidades de SN se proporcionan en nombre de los HEs con los que la SN tiene un acuerdo apropiado. Las responsabilidades de la SN son recoger los cargos y datos de contabilidad y la transferencia de dichos datos a los HEs, así como la interacción y la provisión de facilidades a los HEs para identificar, autenticar, autorizar y localizar a los usuarios.

Las relaciones entre usuarios, SNs y HEs con respecto a la provisión del servicio de red son:

1. Relación usuario-SN . Un usuario obtiene acceso al servicio(s) en UMTS mediante la comunicación con una red SN. La red SN requerirá garantía de que quienquiera que sea el usuario, el HE estará preparado para pagar por el servicio que la SN proporcione al usuario. Análogamente, el usuario necesita garantía de que la red SN proporcionará el servicio pedido a un coste acordado con el usuario y con la calidad de servicio esperada por el usuario. Esto normalmente implicará algún tipo de proceso de autenticación entre el usuario y la red SN que puede o no implicar interacción «en línea» o «fuera de línea» con el HE.

2. Relación usuario-HE . Un usuario está inicialmente registrado con uno o más HEs. Durante este proceso de registro el HE expide al usuario un USIM para utilizar durante el proceso de autenticación y establecimiento de clave.

3. Relación SN-HE . Cuando una red se comunica con un usuario, normalmente será necesario que la red obtenga información relativa al usuario del HE del usuario, esto puede hacerse «en línea» o «fuera de línea» dependiendo del mecanismo. La red también será responsable de proporcionar información de estado relativa al usuario, incluyendo información de localización y datos relacionados con los cargos de vuelta al HE. La integridad de datos y la autenticación del origen normalmente necesitarán ser proporcionados en este tipo de datos de mensajería de almacenamiento y reenvío que se transfiere entre SNs y HEs. Sin embargo, la provisión de dichos servicios de seguridad no se considera parte de la seguridad de acceso a red.

SEGURIDAD EXTREMO A EXTREMO ENTRE USUARIOS Y VASP: ROLES Y SU INTERRELACION

Los «roles» de este tipo de servicio de seguridad son:

(i) Usuario.

(ii) HN (Home Environment).

(iii) VASP. Es el «rol» que proporciona aplicaciones a los usuarios sobre portadores UMTS. Los VASPs pueden ser terceras partes que pueden tener alguna asociación con un HE para cargar y facturar o pueden ser proporcionados por alguna organización que proporciona el HE o la SN. El VASP también puede actuar de forma independiente de cualquier HE de UMTS. En este caso el usuario debería pagar al VASP directamente en vez de hacerlo a través del HE.

Las relaciones entre los usuarios, HEs y VASPs con respecto a la provisión de la seguridad extremo a extremo son:

- Relación usuario-VASP. Un usuario obtiene acceso a los servicios de valor añadido en UMTS comunicándose con un VASP. El VASP requerirá garantía de que quien quiera que sea el usuario, el HE estará preparado para pagar el servicio que el VASP proporciona al usuario. Análogamente, el usuario necesita garantía de que el VASP proporcionará el servicio pedido a un coste acordado con el usuario y con la calidad de servicio esperada por el usuario. Esto normalmente implicará algún tipo de proceso de autenticación entre usuario y el VASP que puede o no implicar interacción «en línea» o «fuera de línea» con el HE.

- Relación usuario-HE.

- Relación VASP-HE. Cuando un VASP se comunica con un usuario normalmente será necesario que el VASP obtenga información relativa al usuario del HE del usuario; esto puede realizarse «en línea» o «fuera de línea» dependiendo del mecanismo. El VASP también puede ser responsable de enviar información de estado de usuario y datos relacionados con los cargos, de vuelta al HE. La integridad de datos y la autenticación de origen normalmente se necesitará proporcionar sobre los datos de mensajería de almacenamiento y reenvío transferidos entre VASPs y HEs. Sin embargo, la provisión de dichos servicios no está considerado como parte de la seguridad de acceso a red.

SEGURIDAD EXTREMO A EXTREMO ENTRE USUARIOS: ROLES Y SU INTERRELACIÓN

Los roles identificados son:

- (i) Usuario.
- (ii) HE.

Las relaciones entre estos «roles» son:

(a) Relación usuario-HE.

(b) Relación usuario-usuario. Dos usuarios desearán establecer comunicaciones seguras entre sí. Estos usuarios pueden no haber tenido ninguna relación de confianza previa o asociación de seguridad entre sí pero depositan su confianza en sus respectivos HEs y cualquier relación de confianza relevante entre sus HEs.

(c) Relación HE-HE. Los HE individuales normalmente tendrán alguna clase de relación de confianza y asociación de seguridad entre sí para facilitar las comunicaciones seguras extremo a extremo entre sus usuarios.

FUNCIONALIDAD TTP EN UMTS. TIPOS DE TTPs

La figura 3 muestra la inter-relación entre usuarios, abonados, proveedores de servicio y operadores de red. El esquema de TTP(s) se muestra como entidades externas a UMTS para proporcionar seguridad en los servicios relacionados con las entidades definidas dentro de UMTS. Dentro de UMTS las entidades que requieren un servicio basado en TTP pueden clasificarse en: usuarios, abonados, proveedores de servicios, operadores de red, autoridades nacionales, reguladores.

Las autoridades nacionales y reguladores interactúan con todas las demás partes implicadas en aplicar el funcionamiento legal e imparcial del servicio de telecomunicaciones. Una de las ventajas de las técnicas de seguridad basadas en TTPs es que pueden resolver conflictos de necesidades entre diferentes entidades. Por ejemplo, los conflictos que existen entre las necesidades de los usuarios en cuanto a privacidad, las necesidades de los proveedores en cuanto a seguridad comercial y la demanda de las autoridades nacionales de capacidades de escucha/intercepción.

Una red de TTPs que pueda proporcionar servicios a UMTS debería tener claros beneficios en la provisión de servicios de seguridad extremo a extremo. Con la aparición de nuevos operadores y proveedores de servicios existe una necesidad de relaciones de confianza bien definidas entre las entidades. Una red europea de TTPs permitiría que esta necesidad se cumpla más fácilmente eliminando la necesidad de que las entidades establezcan acuerdos de confianza de forma individual. Igualmente, una red europea de TTPs resolvería los problemas asociados con la itinerancia inter-operador que probablemente se haga más común con el advenimiento de UMTS.

Las TTPs pueden clasificarse de acuerdo a sus relaciones de comunicación con las entidades que sirven. La localización de las TTPs influirá en los servicios que podrán realizar. Las TTPs se pueden clasificar en tres

categorías: i) TTP «on-line». Una TTP de este tipo no se encuentra situada en el camino de comunicación entre las dos entidades. Sin embargo, es requerida por una o ambas entidades en tiempo real para proporcionar o registrar información relativa a la seguridad; ii) TTP «in-line». Este tipo de TTP se coloca en el camino de comunicación entre las dos entidades. Dicha disposición permite a la TTP ofrecer un amplio grupo de servicios de seguridad directamente a los usuarios. Ya que la TTP interrumpe el camino de comunicación, pueden existir en cada extremo diferentes dominios de seguridad, y iii) TTP «off-line». Este tipo de TTP no interactúa con las entidades durante el proceso del servicio de seguridad dado. La interacción se realiza «fuera de línea» para gestionar los datos asociados con el servicio.

ASPECTOS FINALES

Con la creciente cercanía de la implantación de las redes inalámbricas 3G y la convergencia de voz, datos y vídeo, el nuevo enfoque de red UMTS está preparado para proporcionar mayores velocidades de datos y servicios multimedia. UMTS será capaz de entregar un conjunto completo de nuevos servicios con una experiencia de usuario final mejorada. Junto con la convergencia de las redes, existirán dispositivos finales de usuario multifuncionales y mejorados que permitirán nuevas aplicaciones y abrirán segmentos de mercado nuevos (por ejemplo para redes de área personal). Pero en todo esto el Factor Seguridad debe estar presidiendo todos los beneficios que de hecho aporta a todos los agentes implicados: consumidores, comercios, usuarios, operadores de red, abonados, proveedores de servicios, etc. ■

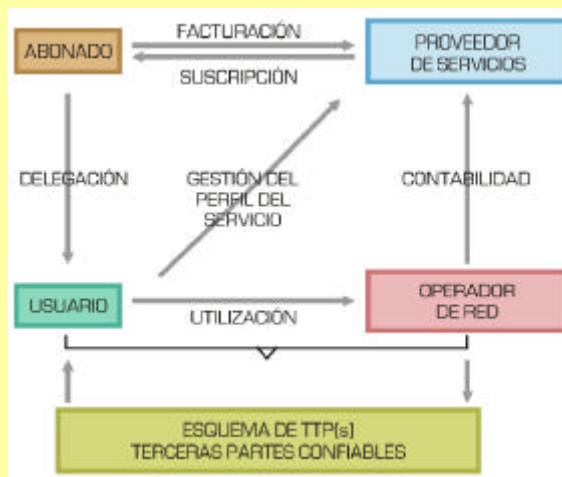


Fig. 3.- Esquema de la relación entre usuarios, abonados, proveedores de servicios, operadores de red y su interacción con un esquema de TTP(s).

Prof. Dr. Javier Areitio Bertolin
Catedrático de la Facultad de Ingeniería. ESIDE
Director del Grupo de Investigación Redes y Sistemas
UNIVERSIDAD DE DEUSTO
jareitio@orion.deusto.es

BIBLIOGRAFÍA

- Areitio, J. «Problemas de Seguridad en el Despliegue de Servicios de Comercio Electrónico a través de Telefonía Celular». Congreso Securmática 2000. Abril 2000. Madrid.
- Areitio, J. «Riesgos de la Seguridad en E-Business a través de la Telefonía Celular». Seminario Internacional de Seguridad en E-Business. ISoft.-EIM/European Institute of Management-Iberdrola. Septiembre 2000. Bilbao.
- Areitio, J. «Comunicaciones móviles digitales celulares: aplicación de la tecnología criptográfica». Grupo CEP Communications. Mayo 1999.
- ETSI. www.etsi.org.
- ITU-TSS. www.itu.org.